United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2009

AVIATION SECURITY

A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls

GAO

Accountability ★ Integrity ★ Reliability

GAO-09-399

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-09-399, a report to congressional requesters

September 2009

AVIATION SECURITY

A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls

Why GAO Did This Study

Incidents of airport workers using access privileges to smuggle weapons through secured airport areas and onto planes have heightened concerns regarding commercial airport security. The Transportation Security Administration (TSA), along with airports, is responsible for security at TSA-regulated airports. To guide risk assessment and protection of critical infrastructure, including airports, the Department of Homeland Security (DHS) developed the National Infrastructure Protection Plan (NIPP). GAO was asked to examine the extent to which, for airport perimeters and access controls, TSA (1) assessed risk consistent with the NIPP; (2) implemented protective programs, and evaluated its worker screening pilots; and (3) established a strategy to guide decision making. GAO examined TSA documents related to risk assessment activities, airport security programs, and worker screening pilots; visited nine airports of varying size; and interviewed TSA, airport, and association officials.

What GAO Recommends

GAO recommends, among other things, that TSA develop a comprehensive risk assessment of airport security, and milestones for its completion; an evaluation plan for any future airport security pilot programs; and a national strategy for airport security that includes key characteristics, such as goals and priorities. DHS reviewed a draft of this report and concurred with these recommendations.

View GAO-09-399 or key components.
For more information, contact Steve Lord at (202) 512-4379 or lords@gao.gov.

What GAO Found

Although TSA has implemented activities to assess risks to airport perimeters and access controls, such as a commercial aviation threat assessment, it has not conducted vulnerability assessments for 87 percent of the nation's approximately 450 commercial airports or any consequence assessments. As a result, TSA has not completed a comprehensive risk assessment combining threat, vulnerability, and consequence assessments as required by the NIPP. While TSA officials said they intend to conduct a consequence assessment and additional vulnerability assessments, TSA could not provide further details, such as milestones for their completion. Conducting a comprehensive risk assessment and establishing milestones for its completion would provide additional assurance that intended actions will be implemented, provide critical information to enhance TSA's understanding of risks to airports, and help ensure resources are allocated to the highest security priorities.

Since 2004, TSA has taken steps to strengthen airport security and implement new programs; however, while TSA conducted a pilot program to test worker screening methods, clear conclusions could not be drawn because of significant design limitations and TSA did not document key aspects of the pilot. TSA has taken steps to enhance airport security by, among other things, expanding its requirements for conducting worker background checks and implementing a worker screening program. In fiscal year 2008 TSA pilot tested various methods to screen airport workers to compare the benefits, costs, and impacts of 100 percent worker screening and random worker screening. TSA designed and implemented the pilot in coordination with the Homeland Security Institute (HSI), a federally funded research and development center. However, because of significant limitations in the design and evaluation of the pilot, such as the limited number of participating airports—7 out of about 450—it is unclear which method is more cost-effective. TSA and HSI also did not document key aspects of the pilot's design, methodology, and evaluation, such as a data analysis plan, limiting the usefulness of these efforts. A well-developed and well-documented evaluation plan can help ensure that pilots generate needed performance information to make effective decisions. While TSA has completed these pilots, developing an evaluation plan for future pilots could help ensure that they are designed and implemented to provide management and Congress with necessary information for decision making.

TSA's efforts to enhance the security of the nation's airports have not been guided by a unifying national strategy that identifies key elements, such as goals, priorities, performance measures, and required resources. For example, while TSA's various airport security efforts are implemented by federal and local airport officials, TSA officials said that they have not identified or estimated costs to airport operators for implementing security requirements. GAO has found that national strategies that identify these key elements strengthen decision making and accountability; in addition, developing a strategy with these elements could help ensure that TSA prioritizes its activities and uses resources efficiently to achieve intended outcomes.

Contents

Tables

Figures

Abbreviations

AACPP	Airport Access Control Pilot Program
ACIS	Aviation Credential Interoperability Solution
ADASP	Aviation Direct Access Screening Program
ADRA	air domain risk assessment
APS	Airport Perimeter Security
ASP	Airport Security Program
AOA	air operations area
ATSA	Aviation and Transportation Security Act
CHRC	criminal history records check
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FSD	federal security director
GPRA	Government Performance and Results Act
HSI	Homeland Security Institute
HSPD	Homeland Security Presidential Directive
NIPP	National Infrastructure Protection Plan
JVA	joint vulnerability assessment
OIG	Office of Inspector General
OMB	Office of Management and Budget
SIDA	security identification display area
SPOT	Screening of Passengers by Observation Techniques
STA	security threat assessment
TSA	Transportation Security Administration
TSOB	Transportation Security Oversight Board
TS-SSP	Transportation Systems-Sector Specific Plan
VIPR	Visible Intermodal Prevention and Response

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 30, 2009

Congressional Requesters

Recent criminal incidents involving airport workers using their access privileges to smuggle weapons and drugs into secured areas of commercial airports and onto planes has heightened concerns about the risks posed by workers and the security of airport perimeters and access to secured areas.[1] Moreover, the Transportation Security Administration (TSA), the agency primarily responsible for securing the nation's civil aviation system,[2] has identified workers with access to secured airport areas as one of the greatest potential threats to aviation and highlighted the need to keep airport perimeters secure.[3] Pursuant to the Aviation and Transportation Security Act (ATSA), which was signed into law shortly after the terrorist attacks of September 11, 2001, TSA assumed primary responsibility for implementing and overseeing security operations within the nation's civil aviation system.[4] This includes overseeing U.S. airport operator efforts to maintain and improve the security of perimeters and the access controls, as well as implementing measures to reduce risks posed by workers at the nation's commercial airports.[5] While airport operators, not TSA, generally retain direct day-to-day operational

[1] See, for example, Department of Homeland Security, Office of the Inspector General, *TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening (Revised for Public Disclosure)*, OIG-09-05 (Washington, D.C., Oct. 28, 2008).

[2] In general, civil aviation includes all nonmilitary aviation operations, including scheduled and chartered air carrier operations, cargo operations, and general aviation, as well as the airports servicing these operations (including commercial airports).

[3] Access controls can include security measures such as pedestrian and vehicle gates, keypad access codes that use personal identification numbers, magnetic stripe cards and readers, fingerprint readers or other biometric technology, turnstiles, locks and keys, and security personnel.

[4] See Pub. L. No. 107-71, 115 Stat. 597 (2001).

[5] In this report, "airport workers" refers to any individuals employed at an airport who require access to areas not otherwise accessible by the general traveling public, including individuals directly employed by the airport operator as well as individuals employed by retail, air carrier, maintenance, custodial, or other entities operating on airport property. In addition, "airport security" refers specifically to airport perimeter and access control security, which we use interchangeably, and "commercial airport" refers to a U.S. airport operating under a TSA-approved security program that services air carriers with regularly scheduled passenger operations.

responsibility for these areas of security, TSA is responsible for establishing and implementing measures to improve the security of airport perimeters and access controls to secured areas within the airports and to reduce the security risks posed by airport workers.

In 2004 we reported that TSA had taken steps to enhance the security of airport perimeters and access controls, but that it faced challenges in identifying security weaknesses of the commercial airport system, prioritizing funding to address the most critical security needs, and taking steps to reduce the risks posed by airport workers.[6] We recommended, among other things, that TSA determine if and when additional security requirements are needed to reduce the risks posed by airport workers. TSA generally concurred with our findings and recommendations and has taken steps to address these recommendations.

Since it is not feasible to protect all assets and systems against every possible threat, the Department of Homeland Security (DHS) has called for using a risk management approach to prioritize its investments, develop plans, and allocate resources in a risk-informed way that balances security and commerce.[7] Risk management calls for a cost-effective use of resources and focuses on developing and implementing protective actions that offer the greatest mitigation of risk for any given expenditure. A risk management approach entails a continual process of managing risk through a series of actions, including setting goals and objectives, assessing risk, evaluating alternatives, selecting initiatives to undertake, and implementing and monitoring those initiatives. In 2009 DHS updated the National Infrastructure Protection Plan (NIPP), which names TSA as the primary federal agency responsible for coordinating critical infrastructure protection efforts within the transportation sector and establishes a risk management framework to guide security decisions.[8]

[6] GAO, *Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls*, GAO-04-728 (Washington, D.C.: June 4, 2004).

[7] In the context of risk management, "risk-based" and "risk-informed" are often used interchangeably to describe the related decision-making processes. However, according to the DHS Risk Lexicon, risk-based decision making uses the assessment of risk as the primary decision driver, while risk-informed decision making may consider other relevant factors in addition to risk assessment information. Because it is an acceptable DHS practice to use other information in addition to risk assessment information to inform decisions, we have used "risk-informed" throughout this report.

[8] The NIPP provides a unifying structure for the integration of a range of efforts for the protection and resilience of the nation's critical infrastructure and key resources.

To respond to the threat posed by airport workers, the Explanatory Statement accompanying the DHS Appropriations Act, 2008, directed that TSA use $15 million of its appropriation to conduct a pilot program to help identify the potential costs and benefits of 100 percent worker screening and other worker screening methods.[9] TSA worked with airport stakeholders to develop the program, and in May 2008 began to test various methods of screening workers—including 100 percent worker screening—at seven airports located throughout the nation. TSA issued a final report on the results of the pilot program in July 2009.[10]

You requested that we examine TSA's actions since 2004 to strengthen the security of commercial airport perimeters and access to secured airport areas. This report evaluates to what extent TSA has

- assessed the risk to airport security consistent with the NIPP risk management framework;
- implemented protective programs to strengthen airport security, and evaluated its worker screening pilot program; and
- established a national strategy to guide airport security decision making.

To conduct our review, we examined documents related to TSA's risk assessment and security activities and programs with regard to airport security, such as TSA's Civil Aviation Threat Assessment. We also reviewed documents related to TSA's airport perimeter and access controls security–related programs, such as standard operating procedures for the Aviation Direct Access Screening Program (TSA's random worker screening program), as well as relevant laws, presidential directives, and TSA management directives. We compared this information with criteria in DHS's NIPP, the Transportation Systems Sector-Specific Plan (TS-SSP),[11] TSA's risk management methodology, and our prior work

[9] Explanatory Statement accompanying Division E of the Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat. 1844, 2042 (2007). The Statement refers to these pilot projects as airport employee screening pilots. However, for the purposes of this report, we use "worker screening" to refer to the screening of all individuals who work at the airport and require access beyond public areas, such as vendor, airport, air carrier, and maintenance employees. According to TSA, it expended about $8 million to design, implement, and evaluate this pilot program.

[10] Transportation Security Administration, *Airport Employee Screening Pilot Program Study: Fiscal Year 2008 Report to Congress* (Washington, D.C., July 7, 2009).

[11] TSA developed the TS-SSP to conform to NIPP requirements, which required TSA and other sector-specific agencies to develop strategic risk management frameworks for their sectors that aligned with NIPP guidance.

on risk management.[12] We relied on TSA to identify its risk assessment activities for airport security, and we examined how these individual threat and vulnerability assessment activities addressed the security of airport perimeter and access controls. Because of the scope of our work, we did not assess the extent to which each of these activities met the NIPP core criteria for individual threat and vulnerability assessments; however, we examined the extent to which the various types of assessment activities TSA identified, taken together, met the NIPP criteria for completing a comprehensive risk assessment that combines threat, vulnerability, and consequence assessments. We also compared TSA's approach to securing the nation's airport perimeters and access to secured areas with guidance on security strategies and planning that we previously reported.[13] We obtained data from TSA officials on vulnerability assessment activities and, by obtaining information on the processes used to schedule and track these activities, determined the data were sufficiently reliable for the purposes of this report. To better understand how TSA has used this information, we interviewed TSA officials responsible for risk management and security programs related to airport perimeters and access controls. We also collected TSA data on security breaches—any violations of security requirements—at commercial airports; however, TSA could not distinguish the number of breaches related only to airport perimeter and access control security from other types of breaches. By obtaining information on the processes used to collect, tabulate, and assess these data, we determined that the data were sufficiently reliable to present contextual information regarding all breaches to secured areas (including the airport perimeter).

In addition, we asked TSA to identify agency-led activities and programs for strengthening airport security, as well as procedures for developing

[12] GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005); *Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security*, GAO-08-904T (Washington, D.C.: June 25, 2008); and *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation*, GAO-09-492 (Washington, D.C.: Mar. 27, 2009).

[13] In prior work we identified a set of desirable characteristics to aid responsible parties in further developing and implementing national strategies—and to enhance their usefulness in resource and policy decisions and to better ensure accountability. For a more detailed discussion of these characteristics, see GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

and issuing airport perimeter and access control security requirements through security directives. We then assessed and summarized the program information, operations directives, and standard operating procedures provided by TSA to determine if the agency addressed relevant statutory requirements and recommendations from our 2004 report.[14] We also evaluated TSA's final report on its worker screening pilot program, including conclusions and limitations cited by the contractor—the Homeland Security Institute (HSI)—TSA hired to assist with the pilot's design, implementation, and evaluation.[15] Further, we analyzed TSA and HSI's documentation of the pilot program's methodology and implementation, and compared it to criteria in standards for internal control in the federal government and our previous work on pilot program development and evaluation.[16] At our request, TSA identified 25 security directives and emergency amendments that imposed requirements related to airport perimeter and access control security, which we examined to identify specific areas of regulation. To obtain additional information on TSA's efforts to strengthen airport security, we interviewed officials from the two industry associations that support commercial airport operators and their personnel,[17] and conducted site visits at 9 of approximately 450 U.S. commercial airports. During these visits we toured airport facilities and interviewed federal security directors (FSD) and airport security coordinators.[18] We selected these airports based on several factors, including airport size, category,[19] geographical dispersion, and technological initiatives related to airport perimeter and access control

[14] GAO-04-728.

[15] Transportation Security Administration, *Airport Employee Screening Pilot Program Study: Fiscal Year 2008 Report to Congress.*

[16] See GAO, *Internal Control: Standards for Internal Controls in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999), and *Tax Administration: IRS Needs to Strengthen Its Approach for Evaluating the SRFMI Data-Sharing Pilot Program*, GAO-09-45 (Washington, D.C.: Nov. 7, 2008).

[17] According to these industry associations, their combined membership includes thousands of airport management personnel, and represents approximately 95 percent of domestic airline passenger and air cargo traffic in North America.

[18] FSDs are the ranking TSA authorities responsible for leading and coordinating TSA security activities at the nation's more than 450 commercial airports.

[19] TSA classifies the nation's approximately 450 commercial airports into one of five categories (X, I, II, III, and IV) based on various factors, such as the number of take-offs and landings annually, the extent of passenger screening at the airport, and other security considerations. In general, Category X airports have the largest number of passenger boardings, and Category IV airports have the smallest.

security (such as infrared intrusion detection systems). In addition, we conducted interviews with officials from four airports that had voluntarily implemented or were considering implementing additional worker screening methods.[20] While the experiences of these officials and airports cannot be generalized to all airports and security officials, they provided insight into how security efforts were chosen and developed. A more detailed discussion of our scope and methodology is contained in appendix I.

We conducted this performance audit from May 2007 through September 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Airport Security Roles and Responsibilities

On February 17, 2002, pursuant to ATSA, TSA assumed responsibility for the security of the nation's civil aviation system from the Federal Aviation Administration (FAA), including FAA's existing aviation security programs, plans, regulations, orders, and directives covering airports, air carriers, and other related entities. Among other things, ATSA directs TSA to improve the security of airport perimeters and the access controls leading to secured areas, and take measures to reduce the security risks posed by airport workers. (See app. II for more specific details on ATSA requirements and TSA's actions to address these requirements.) TSA has 158 FSDs who oversee the implementation of, and adherence to, TSA requirements at the approximately 450 commercial airports nationwide. As part of TSA's oversight role, it also conducts compliance inspections,[21]

[20] We also discussed with airport officials additional employee screening methods that had been implemented at two of the airports we visited.

[21] On an ongoing basis, TSA must assess and test for compliance with access control requirements. See 49 U.S.C. § 44903(g)(2)(D).

covert testing,[22] and vulnerability assessments to analyze and improve security. (See app. III for information on how TSA uses compliance inspections and covert testing to identify possible airport security vulnerabilities.)

In general, TSA funds its perimeter and access control security–related activities out of its annual appropriation and in accordance with direction set forth in congressional committee reports. For example, the Explanatory Statement accompanying the DHS Appropriations Act, 2008, directed that TSA allocate $15 million of its appropriation to a worker screening pilot program. TSA does not track the amount of funds spent in total for perimeter and access controls because related efforts and activities can be part of broader security programs that also serve other aspects of aviation security. In addition, airports may receive federal funding for perimeter and access control security, such as through federal grant programs or TSA pilot programs. (For more information on such airport security costs and funding, see app. IV.)

Airport operators have direct responsibility for day-to-day aviation operations, including, in general, the security of airport perimeters, access controls, and workers, as well as for implementing TSA security requirements. Airport operators implement security requirements in accordance with their TSA-approved security programs.[23] Elements of a security program may include, among other things, procedures for performing background checks on airport workers, applicable training programs for these workers, and procedures and measures for controlling access to secured airport areas. Security programs may also be required to describe the secured areas of the airport, including a description and map

[22] Covert tests are any test of security systems, personnel, equipment, and procedures to obtain a snapshot of the effectiveness of airport passenger security checkpoint screening, checked baggage screening, and airport access controls to improve airport performance, safety, and security.

[23] Most commercial airports discussed in this report, which are those servicing domestic and foreign air carriers with regularly scheduled passenger operations, operate under "complete" security programs. See 49 C.F.R. § 1542.103(a). "Supporting" and "partial" security programs generally apply to airports servicing smaller air carrier operations and contain fewer requirements. See § 1542.103(b), (c). In general, security programs may be amended, with TSA approval, provided that the proposed amendment provides the requisite level of security, among other things. See § 1542.105.

detailing boundaries and pertinent features of the secured areas, and the measures used to control access to such areas.[24]

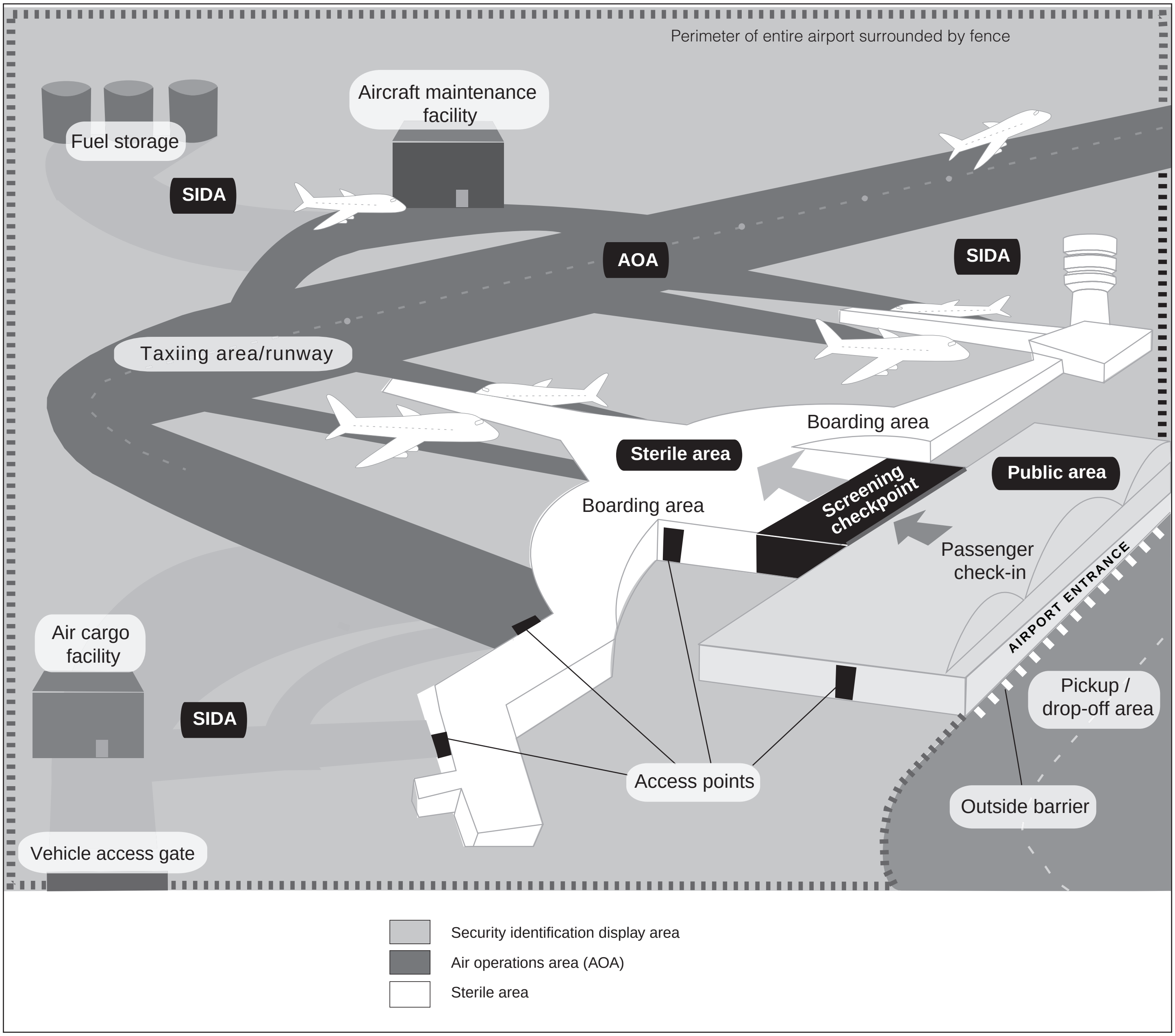
Commercial airports are generally divided into designated areas that have varying levels of security, known as secured areas, security identification display areas (SIDA), air operations areas (AOA), and sterile areas.[25] Sterile areas, located within the terminal, are where passengers wait after screening to board departing aircraft. Access to sterile areas is controlled by TSA screeners at security checkpoints, where they conduct physical screening of passengers and their property.[26] Airport workers may access the sterile area through the security checkpoint or through other access points secured by the airport operator in accordance with its security program. The SIDA and the AOA are not to be accessed by passengers, and typically encompass baggage loading areas, areas near terminal buildings, and other areas close to parked aircraft and airport facilities, as illustrated in figure 1.

[24] See § 1542.103(a).

[25] For the purposes of this report "secured area" is used generally to refer to areas specified in an airport security program that require restricted access, including the SIDA, the AOA, and the sterile area. While security measures governing access to such areas may vary, in general a SIDA is an area in which appropriate identification must be worn, an AOA is an area providing access to aircraft movement and parking areas, and a sterile area provides passengers access to boarding aircraft and is an area to which access is generally controlled by TSA or a private screening entity under TSA oversight. See 49 C.F.R. § 1540.5.

[26] At airports participating in TSA's Screening Partnership Program (SPP), employees of private companies under contract to TSA perform screening operations, with TSA oversight. See 49 U.S.C. § 44920. For more information on the SPP, see GAO, *Aviation Security: TSA's Cost and Performance Study of Private-Sector Airport Screening*, GAO-09-27R (Washington, D.C: Jan. 9, 2009).

Figure 1: Commercial Airport Areas Typically Have Varying Levels of Security



Source: GAO.

Notes: This figure shows airport security areas designated in accordance with TSA requirements. Pursuant to 49 C.F.R. § 1542.205, each airport area defined as a secured area in a security program must be a SIDA, though other areas of the airport may also be designated as SIDAs by the airport operator. For example, some airport operators designate all AOAs as SIDAs.

Securing access to the sterile area from other secured areas—such as the SIDA—and security within the area, is the responsibility of the airport operator, in accordance with its security program. Airport perimeter and access control security is intended to prevent unauthorized access into secured areas—either from outside the airport complex or from within the airport's sterile area. Individual airport operators determine the boundaries for each of these areas on a case-by-case basis, depending on the physical layout of the airport and in accordance with TSA requirements. As a result, some of these areas may overlap. Within these areas, airport operators are responsible for safeguarding their airfield barriers, preventing and detecting unauthorized entry into secured areas, and conducting background checks of workers with unescorted access to secured areas.

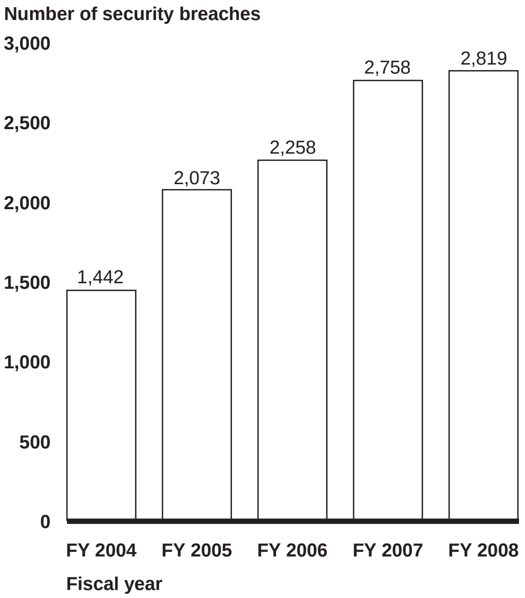
Methods used by airports to control access through perimeters or into secured areas vary because of differences in the design and layout of individual airports, but all access controls must meet minimum performance standards in accordance with TSA requirements. These methods typically involve the use of one or more of the following: pedestrian and vehicle gates, keypad access codes using personal identification numbers, magnetic stripe cards and readers, turnstiles, locks and keys, and security personnel.

According to TSA officials, airport security breaches occur within and around secured areas at domestic airports (see fig. 2 for the number of security breaches reported by TSA from fiscal year 2004 through fiscal year 2008). While some breaches may represent dry runs by terrorists or others to test security or criminal incidents involving airport workers, most are accidental.[27] TSA requires FSDs to report security breaches that occur both at the airports for which they are responsible and on board aircraft destined for their airports. TSA officials said that they review security breach data and report them to senior management as requested,

[27] According to a TSA official, a breach of security does not necessarily mean that a threat existed or was successful. The significance of a breach must be considered in light of several factors, including the intent of the perpetrator and whether existing security measures and procedures successfully responded to, and mitigated against, the breach so that no harm to persons, facilities, or other assets resulted.

and provide data on serious breaches to senior management on a daily basis, as applicable.

Figure 2: Total Number of TSA-Reported Security Breaches from Fiscal Years 2004 through 2008



Source: GAO analysis of TSA data.

Notes: Because these data include security breaches that occurred within any type of secured area, including sterile areas frequented by passengers, they are not specific to perimeter and access controls and cannot be analyzed to identify trends related to breaches solely related to perimeter and access control security. At the time of our review, TSA officials told us that they were unable to identify how much of the increase in breaches could be specifically related to airport workers or to the security of airport perimeters and access controls. Finally, the data are based on total breaches and have not been adjusted to reflect potential issues that could influence how the data are interpreted, such as annual increases in passenger volume, changes in the number of commercial airports, or significant variations in the number of breaches at individual airports.

According to a TSA official, the increase in known breaches from fiscal years 2004 through 2005 reflects a change in the requirements for reporting security breaches that TSA issued in December 2005.[28] This

[28] Transportation Security Administration, *Reporting Security Incidents Via PARIS*, Operations Directive OD-400-18-1 (Washington, D.C., Dec. 16, 2005). According to TSA officials, these reporting requirements (1) allow FSDs to better distinguish between different types of security breaches and other incidences, (2) reflect changes in data collection methods, and (3) provide for greater accuracy in the reporting of security incidences.

change provided more specific instructions to FSDs on how to categorize different types of security incidents. Regarding increases in security breaches from fiscal years 2005 through 2008, TSA officials said that while they could not fully explain these increases, there could be several reasons to account for this growth. For example, according to TSA officials, changes in TSA management often trigger increases in specific types of breaches reported, such as since 2004, when the priorities of the new Administrator resulted in an increase in the reporting of restricted items. TSA officials also stated that a report of a security breach at a major U.S. airport is likely to cause security and law enforcement officials elsewhere to subsequently raise the overall awareness of security requirements for a period of time. In addition, TSA noted that certain inspections conducted by TSA officials tend to produce heightened awareness by federal and airport employees whose perimeter security and access control procedures are being inspected for compliance with regulations.

Risk Management Approach Can Help Guide Homeland Security Efforts

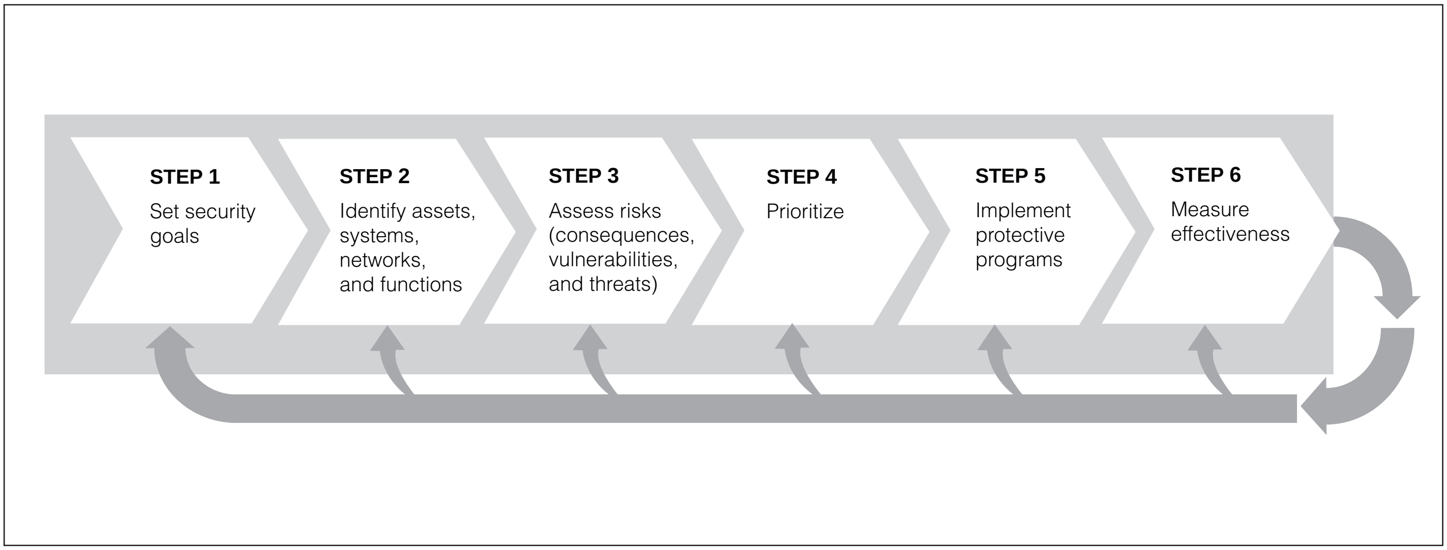
Risk management is a tool for informing policymakers' decisions about assessing risks, allocating resources, and taking actions under conditions of uncertainty. We have previously reported that a risk management approach can help to prioritize and focus the programs designed to combat terrorism.[29] Risk management, as applied in the transportation security context, can help federal decision makers determine where and how to invest limited resources within and among the various modes of transportation.[30] In accordance with Homeland Security Presidential Directive (HSPD) 7, the Secretary of Homeland Security designated TSA as the sector-specific agency for the transportation security sector, requiring TSA to identify, prioritize, and coordinate the protection of critical infrastructure and key resources within this sector and integrate risk

[29] See GAO-09-492, and GAO, *Commercial Vehicle Security: Risk-Based Approach Needed to Secure the Commercial Vehicle Sector*, GAO-09-85 (Washington, D.C.: Feb. 27, 2009); *Highway Infrastructure: Federal Efforts to Strengthen Security Should Be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure*, GAO-09-57 (Washington, D.C.: Jan. 30, 2009); *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-07-225T (Washington, D.C.: Jan. 18, 2007); and *Transportation Security: Systematic Planning Needed to Optimize Resources*, GAO-05-357T (Washington, D.C.: Feb. 15, 2005).

[30] "Modes of transportation" refers to the different means that are used to transport people or cargo. There are six modes of transportation: aviation, maritime, mass transit, highway, freight rail, and pipeline.

management strategies into its protective activities.[31] In June 2006, in accordance with HSPD-7 and the Homeland Security Act of 2002, DHS released the NIPP, which it later updated in 2009. The NIPP developed a risk management framework for homeland security. In accordance with the NIPP, TSA developed the TS-SSP to govern its strategy for securing the transportation sector, as well as annexes for each mode of transportation, including aviation. The NIPP and TS-SSP set forth risk management principles, including a comprehensive risk assessment process for considering threat, vulnerability, and consequence assessments to determine the likelihood of terrorist attacks and the severity of the impacts. Figure 3 illustrates the interrelated activities of the NIPP's risk management framework.

Figure 3: NIPP Risk Management Framework


STEP 1
Set security goals
STEP 2
Identify assets, systems, networks, and functions
STEP 3
Assess risks (consequences, vulnerabilities, and threats)
STEP 4
Prioritize
STEP 5
Implement protective programs
STEP 6
Measure effectiveness

Sources: GAO presentation of DHS information.

- **Set security goals:** Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture.

[31] HSPD-7 specifically directed the Departments of Transportation and Homeland Security to collaborate on all matters relating to transportation security and transportation infrastructure protection.

- **Identify assets, systems, networks, and functions:** Develop an inventory of the assets, systems, and networks that constitute the nation's critical infrastructure, key resources, and critical functions. Collect information pertinent to risk management that takes into account the fundamental characteristics of each sector.

- **Assess risks:** Determine risk by combining potential direct and indirect consequences of a terrorist attack or other hazards (including seasonal changes in consequences and dependencies and interdependencies associated with each identified asset, system, or network), known vulnerabilities to various potential attack vectors, and general or specific threat information.[32]

- **Prioritize:** Aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk; establish priorities based on risk; assess the mitigation of risk for each proposed activity based on a specific investment; and determine protection and business continuity initiatives that provide the greatest mitigation of risk.

- **Implement protective programs:** To reduce or manage identified risk, select sector-appropriate protective actions or programs that offer the greatest mitigation of risk for any given resource/expenditure/investment. Secure the resources needed to address priorities.

- **Measure effectiveness:** Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of the national Critical Infrastructure and Key Resources Protection Program in improving protection, managing risk, and increasing resiliency.[33]

[32] In the context of the NIPP, risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. The NIPP framework calls for risk to be assessed from any scenario as a function of threat, vulnerability, and consequence. Once the three components of risk have been assessed, they must be integrated into a defensible model to produce a risk estimate. The NIPP allows an agency to determine whether to assess the risk to an asset, system, network, or function, depending on the characteristics of the infrastructure being examined. TSA has adopted a systems-based approach to risk assessment.

[33] According to the NIPP, the national Critical Infrastructure and Key Resources Protection Program is designed to reduce the vulnerability of critical infrastructure and key resources in order to deter and mitigate terrorist attacks. The program identifies, prioritizes, and coordinates the protection of critical infrastructure and key resources with an emphasis on those that could be exploited to cause catastrophic health effects or mass casualties, which would be comparable to those resulting from a weapon of mass destruction.

Within the risk management framework, the NIPP also establishes core criteria for risk assessments. According to the NIPP, risk assessments are a qualitative determination, a quantitative determination, or both of the likelihood of an adverse event occurring and are a critical element of the NIPP risk management framework. Risk assessments also help decision makers identify and evaluate potential risks so that countermeasures can be designed and implemented to prevent or mitigate the potential effects of the risks. The NIPP characterizes risk assessment as a function of three elements:

- **Threat:** The likelihood that a particular asset, system, or network will suffer an attack or an incident. In the context of risk associated with a terrorist attack, the estimate of this is based on the analysis of the intent and the capability of an adversary; in the context of a natural disaster or accident, the likelihood is based on the probability of occurrence.

- **Vulnerability:** The likelihood that a characteristic of, or flaw in, an asset's, system's, or network's design, location, security posture, process, or operation renders it susceptible to destruction, incapacitation, or exploitation by terrorist or other to intentional acts, mechanical failures, and natural hazards.

- **Consequence:** The negative effects on public health and safety, the economy, public confidence in institutions, and the functioning of government, both direct and indirect, that can be expected if an asset, system, or network is damaged, destroyed, or disrupted by a terrorist attack, natural disaster, or other incident.

Information from the three elements used in assessing risk—threat, vulnerability, and consequence—can lead to a risk characterization and provide input for prioritizing security goals.

TSA Has Taken Steps to Assess Threats and Vulnerabilities for Airport Security, but Has Not Conducted a Comprehensive Risk Assessment to Help Identify Priorities and Allocate Resources

While TSA has taken steps to assess risk, it has not conducted a comprehensive risk assessment based on assessments of threats, vulnerabilities, and consequences. TSA officials reported that they have identified threats to airport security as part of an overall assessment of threats to the civil aviation system. While TSA has conducted vulnerability assessment activities at select airports, it has not analyzed whether the select assessments reflect the overall vulnerability of airport security nationwide. Further, TSA has not yet assessed the consequences of an attack against airport perimeter and access control security.

TSA Has Taken Steps to Assess Risk, but a Comprehensive Risk Assessment Would Identify Priorities and Inform Resource Allocation

According to the NIPP, risk assessments are to be documented, reproducible (so that others can verify the results), defensible (technically sound and free of significant errors), and complete. The NIPP maintains that these qualities are necessary to risk assessments so they can be used to support national-level, comparative risk assessment, planning, and resource prioritization. For a risk assessment to be considered complete, the NIPP states that it must specifically assess threat, vulnerability, and consequence; after these three components have been assessed, they are to be combined to produce a risk estimate.[34] According to the NIPP, comprehensive risk assessments are necessary for determining which assets or systems face the highest risk for prioritizing risk mitigation efforts and the allocation of resources and for effectively measuring how security programs reduce risks.

In March 2009 we reported that a lack of information that fully depicts threats, vulnerabilities, and consequences limits an organization's ability to establish priorities and make cost-effective security measure decisions.[35] TSA officials told us that they have not completed a comprehensive risk assessment for airport security, although they said that they have prepared

[34] As updated in 2009, the NIPP states that to be complete a risk assessment is to assess threat, vulnerability, and consequence for every defined risk scenario. However, because the original 2006 version of the NIPP described risk assessments that included all three components as "credible," our previous reports use this term rather than "complete" (e.g., see GAO-09-492).

[35] See GAO-09-492.

and are currently reviewing a draft of a comprehensive, scenario-based air domain risk assessment (ADRA), which officials said is to serve as a comprehensive risk assessment for airport security.[36] According to officials, the ADRA is to address all three elements of risk for domestic commercial aviation, general aviation, and air cargo.[37] However, TSA has not released it as originally planned for in February 2008. As of May 2009 TSA officials had not provided revised dates for when the agency expects to finalize the ADRA, and they could not provide documentation to demonstrate to what extent the ADRA will address all three components of risk for airport perimeter and access control security. As a result, it is not clear whether the ADRA will provide the risk analysis needed to inform TSA's decisions and planning for airport perimeter and access control security.[38] Standard practices in program management call for documenting the scope of the program and milestones (i.e., time frames) to ensure results are achieved.[39] Conducting a comprehensive risk assessment for airport security and documenting milestones for its implementation would help ensure that TSA's intended actions will be implemented, and would allow TSA to more confidently ensure that its investments in airport security are risk informed and allocated toward the highest-priority risks.

[36] The ADRA is part of TSA's effort to meet the requirements of HSPD-16, *National Strategy for Aviation Security*, which assigned roles and responsibilities to federal stakeholders, including the Secretaries of Homeland Security, State, Defense, Commerce, Energy, and Transportation; the Attorney General; and the Director of National Intelligence, and called for coordination with state, local, and tribal governments and the private sector, to optimize and integrate governmentwide aviation security efforts.

[37] Commercial aviation includes that sector of the nation's civil aviation system that provides for the transportation of individuals by scheduled or chartered operations for a fee, including air carriers and airports. General aviation encompasses all civil aviation other than commercial and military operations, including flight operations such as personal/family transportation, emergency services, wildlife and land surveys, traffic reporting, agricultural aviation, firefighting, and law enforcement. Air cargo is defined as cargo carried on passenger and all-cargo aircraft.

[38] The ADRA is to have three parts: (1) assessments of over 130 terrorist attack scenarios and the extent to which they pose a threat, (2) assessments of known vulnerabilities through which these terrorist attacks could be carried out, and (3) assessments of the consequences of the attack scenarios. TSA officials stated that the primary source for the scenarios included professional judgment of subject matter experts, intelligence information on potential threats, and other information.

[39] The Project Management Institute, *The Standard for Program Management©* (Newtown Square, Penn., 2006).

TSA Uses a Variety of Products to Assess Threat to Airport Security

A threat assessment is the identification and evaluation of adverse events that can harm or damage an asset.[40] TSA uses several products to identify and assess potential threats to airport security, such as daily intelligence briefings, weekly suspicious incident reports, and situational awareness reports,[41] all of which are available to internal and external stakeholders. TSA also issues an annual threat assessment of the U.S. civil aviation system, which includes an assessment of threats to airport perimeter and access control security. According to TSA officials, these products collectively form TSA's assessment of threats to airport perimeter and access control security. TSA's 2008 Civil Aviation Threat Assessment cites four potential threats related to perimeter and access control security, one of which is the threat from insiders—airport workers with authorized access to secured areas.[42] The 2008 assessment characterized the insider threat as "one of the greatest threats to aviation,"[43] which TSA officials explained is meant to reflect the opportunity insiders have to do damage, as well as the vulnerability of commercial airports to an insider attack, which these officials stated as being very high.[44] As of May 2009, TSA had no knowledge of a specific plot by terrorists or others to breach the security of any domestic commercial airport. However, TSA has also noted that airports are seen as more accessible targets than aircraft, and that

[40] For the purposes of estimating risk, according to the NIPP, the threat of an intentional adverse event is generally estimated as the likelihood of such an event; in the case of terrorist attacks, the likelihood is estimated based on the intent and capability of the adversary.

[41] Daily intelligence briefings include a 24-hour snapshot of transportation-related intelligence based on TSA operational reports and other sources. These briefings are used internally by TSA and by other agencies. TSA also provides weekly analysis of suspicious activities and surveillance directed against all transportation modes, which it disseminates within the agency and to other law enforcement agencies. In addition, TSA provides in-depth analysis on specific topics within transportation modes, which may be used to provide situational awareness of an ongoing or recent event.

[42] Transportation Security Administration, *Civil Aviation Threat Assessment* (Washington, D.C., Dec. 30, 2008). The other three threat types discussed in the 2008 assessment are the threat from standoff weapons (such as antitank weapons), which pose a threat to the AOA; the threat from outside the airport perimeter; and the threat of a perimeter breach, which terrorists may see as an attractive target.

[43] TSA's 2007 Threat Assessment also included this conclusion of the insider threat, and the 2006 Threat Assessment characterized the insider threat as "very dangerous." According to the 2008 assessment, the insider is considered extremely difficult to counter because of the individual's position of trust.

[44] According to TSA officials, the risk that insiders will do damage to an airport or aircraft—which they refer to as insider risk—is perceived as both a threat and vulnerability.

airport perimeters may become more desirable targets as terrorists look for new ways to circumvent aviation security.

Intelligence is necessary to inform threat assessments. As we reported in March 2009,[45] TSA has not clarified the levels of uncertainty—or varying levels of confidence—associated with the intelligence information it has used to identify threats to the transportation sector and guide its planning and investment decisions. Both Congress and the administration have recognized uncertainty inherent in intelligence analysis, and have required analytic products within the intelligence community to properly caveat and express uncertainties or confidence in resulting conclusions or judgments.[46] As a result, the intelligence community and the Department of Defense have adopted this practice in reporting threat intelligence. Since TSA does not assign confidence levels to its analytic judgments, it is difficult for TSA to correctly prioritize its tactics and investments based on uncertain intelligence. In March 2009 we recommended that TSA work with the Director of National Intelligence to determine the best approach for assigning uncertainty or confidence levels to analytic intelligence products and apply this approach.[47] TSA agreed with this recommendation and said that it has begun taking action to address it.

[45] GAO-09-492.

[46] See Pub. L. No. 108-458, § 1019, 118 Stat. 3638, 3671-72 (2004) (requiring the Director of National Intelligence to assign an individual or entity with responsibility for ensuring that finished intelligence products produced by any element or elements of the intelligence community, which includes the Federal Bureau of Investigation, Central Intelligence Agency, and Defense Intelligence Agency, are timely, objective, independent of political consideration, and employ the standards of proper analytic tradecraft). See also Intelligence Community Directive 203 (June 2007) (establishing the Intelligence Community Analytic Standards). The directive provides that each analytic product "properly caveats and expresses uncertainties or confidence in analytic judgments. Analytic products should indicate both the level of confidence in analytic judgments and explain the basis for ascribing it. Sources of uncertainty—including information gaps and significant contrary reporting—should be noted and linked logically and consistently to confidence levels in judgments. As appropriate, products should also identify indicators that would enhance or reduce confidence or prompt revision of existing judgments."

[47] GAO-09-492.

Additional Analysis Could Help Inform TSA's Assessment Activities for Airport Security Vulnerabilities

Analyzing the Extent to Which Joint Vulnerability Assessments Provide an Assessment of Nationwide Vulnerabilities Could Strengthen TSA's Ability to Mitigate Risk

The NIPP requires that a risk assessment include a comprehensive assessment of vulnerabilities in assets or systems, such as a physical design feature or type of location, that make them susceptible to a terrorist attack.[48] As we reported in June 2004,[49] these assessments are intended to facilitate airport operators' efforts to comprehensively identify and effectively address perimeter and access control security weaknesses. TSA officials told us that their primary measures for assessing the vulnerability of commercial airports to attack are the collective results of joint vulnerability assessments (JVA) and professional judgment. TSA officials said that the agency plans to expand the number of JVAs conducted in the future but, as of May 2009, did not have a plan for doing so.

According to TSA officials, JVAs are assessments that teams of TSA special agents and other officials conduct jointly with the Federal Bureau of Investigation (FBI) and, as required by law, are generally conducted every 3 years for airports identified as high risk.[50] In response to our 2004 recommendation that TSA establish a schedule and analytical approach for completing vulnerability assessments for evaluating airport security, TSA developed criteria to select and prioritize airports as high-risk for

[48] The NIPP states that this analysis is to also take into consideration factors such as protective measures that are in place that may reduce the risk of an attack, and is to include estimates of the likelihood of success for each attack scenario.

[49] GAO-04-728.

[50] TSA and the FBI are to conduct joint threat and vulnerability assessments at each high-risk U.S. airport at least every 3 years. See 49 U.S.C. § 44904(a)-(b). See also Pub. L. No. 104-264, § 310, 110 Stat. 3213, 3253 (1996) (establishing the requirement that FAA and the FBI conduct joint threat and vulnerability assessments). Pursuant to ATSA, responsibility for conducting the joint assessments transferred from FAA to TSA. According to FBI officials, the agency's role in JVAs is to develop a national-level threat assessment for each selected airport and provide it to TSA for comparison with the TSA vulnerability assessment, to identify areas of imminent vulnerability.

assessment.[51] TSA officials stated that in addition to assessing airports identified as high risk, the agency has also assessed the vulnerability of other airports at the request of FSDs. According to TSA's TS-SSP, after focusing initially on airports deemed high risk, JVAs are to be conducted at all commercial airports. TSA officials stated that JVA teams assess all aspects of airport security and operations, including fuel, cargo, catering, general aviation, terminal area and law enforcement operations, and the controls that limit access to secured areas and the integrity of the airport perimeter. However, officials emphasized that a JVA is not intended to be a review of an airport's compliance with security requirements and teams do not impose penalties for noncompliance. From fiscal years 2004 through 2008, TSA conducted 67 JVAs at a total of 57 airports[52]—about 13 percent of the approximately 450 commercial airports nationwide. In 2007 TSA officials conducted a preliminary analysis of the results of JVAs conducted at 23 domestic airports during fiscal years 2004 and 2005, and found 6 areas in which 20 percent or more of the airports assessed were identified as vulnerable. Specific vulnerabilities included the absence of blast resistant glass in terminal windows, lack of bollards/barriers in front of terminals, lack of blast resistant trash receptacles, and insufficient electronic surveillance of perimeter lines and access points. As of May 2009 TSA officials said that the agency had not finalized this analysis and, as of that date, did not have plans to do so. TSA officials also told us that they have shared the results of JVA reports with TSA's Office of Security Technology to prioritize the distribution of relevant technology to those airports with vulnerabilities that these technologies could strengthen.

TSA characterizes U.S. airports as a system of interdependent hubs and links (spokes) in which the security of all is affected or disrupted by the security of the weakest one. The interdependent nature of the system necessitates that TSA protect the overall system as well as individual

[51] See GAO-04-728. TSA's criteria give first priority to airports identified as critical infrastructure by DHS's Office of Infrastructure Protection. Second priority is given to airports that are to support a National Security Special Event, such as the Republican or Democratic National Conventions, or an event of national significance (e.g., the Super Bowl). Third priority is given to airports whose FSDs have requested a JVA, or those that TSA Headquarters has identified as needing a JVA. According to TSA officials, FSD requests are usually prompted by changes in airport environment—such as construction—while TSA headquarters requests are in response to specific threats, such as those identified by TSA.

[52] From fiscal years 2004 through 2008, 10 airports received 2 JVAs.

assets.[53] TSA maintains that such a "systems-based approach" allows it to focus resources on reducing risks across the entire system while maintaining cost-effectiveness and efficiency. TSA officials could not explain to what extent the collective JVAs of specific airports constitute a reasonable systems-based assessment of vulnerability across airports nationwide or whether the agency has considered assessing vulnerabilities across all airports. Although TSA has conducted JVAs at each category of airport, 58 of the 67 were at the largest airports.[54] According to TSA data, 87 percent of commercial airports—most of the smaller Category II, III, and IV airports—have not received a JVA.[55] TSA officials said that because they have not conducted JVAs for these airports, they do not know how vulnerable they are to an intentional security breach. In 2004 we reported that TSA intended to compile baseline data on airport security vulnerabilities to enable it to conduct a systematic analysis of airport security vulnerabilities nationwide.[56] At that time TSA officials told us that such analysis was essential since it would allow the agency to determine the adequacy of security policies and help TSA and airport operators better direct limited resources. According to TSA officials, conducting JVAs at all airports would allow them to compile national baseline data on perimeter and access control security vulnerabilities. As of May 2009, however, TSA officials had not yet completed a nationwide vulnerability assessment, evaluated whether the current approach to JVAs would provide the desired systems-based approach to assessing airport security vulnerabilities, or explained why a nationwide assessment or evaluation has not been conducted. In subsequent discussions, TSA officials told us that based on our review they intend to increase the number of JVAs

[53] Transportation Security Administration, "Our Security Strategy: Systems-Based Perspective." TSA characterizes transportation systems as being subject to "cascading failures," where small changes in one part of the system can sometimes lead to large consequences. This is of particular concern in systems like the airport network, which are highly interconnected and interdependent. In the past, terrorists have sought to inflict maximum damage relative to their efforts by attacking parts of the aviation system that would lead to cascading failure.

[54] Of the 67 JVAs conducted at 57 airports from fiscal years 2004 through 2008, 58—or 87 percent—were for Category X and I airports. Of the remaining 9 assessments, 6 were at Category II airports, 1 at a Category III airport, and 2 at Category IV airports.

[55] The category designation of some airports has changed since they received a JVA; in these cases, we used the category designation assigned at the time of the JVA. For the total number of airports in each category, we used TSA data as of June 1, 2009.

[56] See GAO-04-728. We also reported that according to TSA this baseline analysis would allow the agency to determine minimum standards and the adequacy of airport security policies.

conducted at airports that are not categorized as high risk—primarily Category II, III, and IV airports. According to officials, the resulting data are to assist TSA in prioritizing the allocation of limited resources. However, TSA officials could not tell us how many additional airports they plan to assess in total or within each category, the analytical approach and time frames for conducting these assessments, and to what extent these additional assessments, in combination with past JVAs, will constitute a reasonable systems-based assessment of vulnerability across airports nationwide. Standard practices for program management call for establishing a management plan and milestones to meet stated objectives and achieve results.[57] It is also unclear to what extent the ADRA, when it is completed, will represent a systems-based vulnerability assessment, an assessment of airports nationwide, or both. Given that TSA officials believe that the vulnerability of airports to an insider attack is very high and the security of airports is interconnected, this vulnerability would extend throughout the nationwide system of airports. Evaluating the extent to which the agency's current approach assesses systems-based vulnerabilities, including the vulnerabilities of smaller airports, would better position TSA to provide reasonable assurance that it is identifying and addressing the areas of greatest vulnerability and the spectrum of vulnerability across the entire airport system. Further, should TSA decide to conduct a nationwide assessment of airport vulnerability, developing a plan that includes milestones for completing the assessment would help TSA ensure that it takes the necessary actions to accomplish desired objectives within reasonable time frames.

TSA Could Strengthen Its Understanding of Risks by Considering Vulnerability Assessment Activities Conducted by Airport Operators

According to the NIPP, DHS and lead security agencies, such as TSA, are to seek to use information from the risk assessments of security partners, whenever possible, to contribute to an understanding of sector and national risks. Moreover, the NIPP states that DHS and lead agencies are to work together to assist security partners in providing vulnerability assessment tools that may be used as part of self-assessment processes, and provide recommendations regarding the frequency of assessments, particularly in light of emergent threats. According to the NIPP, stakeholder vulnerability assessments may serve as a basis for developing common vulnerability reports that can help identify strategic needs and more fully investigate interdependencies.

[57] Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Third Edition (Newtown Square, Penn., 2006).

However, TSA officials could not explain to what extent they make use of relevant vulnerability assessments conducted independently by airport operators to contribute to the agency's understanding of airport security risks, or have worked with security partners to help ensure that tools are available for airports to conduct self-assessment processes of vulnerability. Officials from two prominent airport industry associations estimated that the majority of airports, particularly larger airports, have conducted vulnerability assessments, although they could not give us a specific number. In addition, officials from 8 of the 10 airports whom we interviewed on this issue told us that their airports had conducted vulnerability assessment activities.[58] Some of these analyses could be useful to TSA in conducting a systematic analysis of airport security vulnerabilities nationwide. By taking advantage, to the extent possible, of existing vulnerability assessment activities conducted by airport operators, TSA could enrich its understanding of airport security vulnerabilities and therefore better inform federal actions for reducing airport vulnerabilities.

TSA Has Not Conducted a Consequence Assessment for Airport Security

According to TSA officials, the agency has not assessed the consequences of a successful attack against airport perimeters or a breach to secured areas within airports, even though the NIPP asserts that the potential consequence of an incident is the first factor to be considered in developing a risk assessment. According to the NIPP, risk assessments should include consequence assessments that evaluate negative effects to public health and safety, the economy, public confidence in national economic and political institutions, and the functioning of government that can be expected if an asset, system, or network is damaged, destroyed, or disrupted by a terrorist attack.

Although TSA officials agree that a consequence assessment for airport security is needed, and have stated that the ADRA is intended to provide a comprehensive consequence assessment based on risk scenarios, the agency has not provided additional details as to what the assessment will include, the extent to which it will assess consequence for airport security, or when it will be completed. Standard management practices call for documenting milestones (i.e., time frames) to ensure that results are

[58] We discussed this issue with officials from seven Category X airports, one Category I airport, one Category II airport, and one Category III airport; however, we did not obtain documentation to verify this information.

achieved.[59] TSA officials have agreed that a consequence assessment for airport perimeter and access controls security is an important element in assessing risk to airport security. In addition, TSA officials commented that although the immediate consequences of a breach of airport security would likely be limited, such an event could be the first step in a more significant attack against an airport terminal or aircraft, or an attempt to use an aircraft as a weapon. Conducting a consequence assessment could help TSA in developing a comprehensive risk assessment and increase its assurance that the resulting steps it takes to strengthen airport security will more effectively reduce risk and mitigate the consequences of an attack on individual airports and the aviation system as a whole.

TSA Has Taken a Variety of Protective Actions to Strengthen Airport Security, but Did Not Follow Accepted Practices in Developing Its Worker Screening Pilot Program; Additionally, Issues Remain regarding Worker Security, Technology, and Other Initiatives

TSA has implemented a variety of programs and protective actions to strengthen airport security, from additional worker screening to assessing different technologies. For example, consistent with the Explanatory Statement, TSA piloted several methods to screen workers accessing secured areas, but clear conclusions could not be drawn because of significant design limitations, and TSA did not develop or document an evaluation plan to guide design and implementation of the pilot. Further, while TSA has strengthened other worker security programs, assessed various technologies, and added to programs aimed at improving general airport security, certain issues, such as whether security technologies meet airport needs, have not been fully resolved.

[59] Project Management Institute, *The Standard for Program Management©*.

TSA Has Taken a Variety of Protective Actions to Improve and Strengthen the Security of Commercial Airports since 2004

TSA has taken a variety of protective actions to improve and strengthen the security of commercial airports through the development of new programs or by enhancing existing efforts. Since we last reported on airport perimeter and access control security in June 2004,[60] TSA has implemented efforts to strengthen worker screening and security programs, improve access control technology, and enhance general airport security by providing an additional security presence at airports. According to TSA, each of its security actions—or layers—is capable of stopping a terrorist attack, but when used in combination (what TSA calls a layered approach), a much stronger system results.[61] To better address the risks posed by airport workers, TSA, in accordance with the Explanatory Statement accompanying the DHS Appropriations Act, 2008, initiated a worker screening pilot program to assess various types of screening methods for airport workers.[62] TSA also implemented a random worker screening program and is currently working to apply its screening procedures consistently across airports. In addition, TSA has expanded its requirements for conducting worker background checks. TSA has also taken steps, such as implementing two pilot programs, to identify and assess technologies to strengthen the security of airport perimeters and access controls to secured areas. Further, TSA has taken steps to strengthen general airport security processes. For example, TSA has developed a program in which teams of TSA officials, law enforcement officers, and airport officials temporarily augment airport security through various actions such as randomly inspecting workers, property, and

[60] GAO-04-728.

[61] Many of TSA's security layers have direct application to airport perimeter and access control security, while some layers apply to other aspects of aviation security, such as hardened cockpit doors, and also to the security of other modes of transportation, such as rail and mass transit. In commenting on a draft of this report, TSA officials noted that in December 2008 the agency implemented "Playbook," a program that authorizes FSDs to carry out variable and unpredictable combinations of operations—or security layers—to address the threat environment at airports. TSA officials consider this program to be an additional layer of security, which is applied to all areas of an airport.

[62] Specifically, the Explanatory Statement directed TSA to pilot various methods for screening airport employees at seven airports, and that all employees be screened at three of the selected airports.

vehicles and patrolling secured areas. Table 1 lists the actions TSA has taken since 2004 to strengthen airport security.[63]

Table 1: Protective Actions TSA Has Taken since 2004 to Strengthen Airport Security

Type of security	TSA program/action	Description
Worker screening pilot test	Pilot program	From May to July 2008, TSA implemented a worker screening pilot program at seven airports that was designed to assess various methods for screening airport workers before they enter secured areas. Three airports tested 100 percent worker screening, and four airports tested a variety of enhanced screening methods, such as random targeted physical inspections.
Worker security programs	Aviation Direct Access Screening Program (ADASP)	Implemented in March 2007, ADASP is an airport worker screening program that is used to enforce access procedures, such as ensuring workers display appropriate credentials and do not possess unauthorized items when entering secure areas. Conducted on an unpredictable basis, ADASP varies in duration and can include temporary worker screening checkpoints, vehicle screening checkpoints, or both.
	Worker background checks	TSA has expanded requirements for background checks and the population of individuals who are subject to these checks. • In July 2004 TSA expanded security threat assessments (STA), which are name-based background checks, to require applicants who would be working in a SIDA or sterile area to submit biographical information, such as date of birth. In 2005 TSA began to require that STAs include a citizenship check. TSA subsequently required STAs for all workers seeking or holding airport-issued identification badges or credentials. • In July 2004 TSA enhanced criminal history records checks (CHRC), which are fingerprint-based background checks, for individuals working in a SIDA or sterile area by requiring applicants seeking unescorted access authority to successfully complete a CHRC. In June 2009, among other things, TSA required airports to renew all airport-identification media every 2 years and to require workers to resubmit biographical information in the event of certain changes.
Security technology	Biometric access control initiatives	TSA has taken steps to respond to statutory requirements related to biometric worker credentialing. • TSA has assisted the aviation industry and a federal aviation advisory committee in developing security standards for biometric access controls. • TSA is in the early stages of developing the Aviation Credential Interoperability Solution program, a standardized credentialing system. Airports will use biometrics to verify the identities of workers and confirm their access privileges before granting them entry to secured areas.

[63] TSA officials told us that the agency has two additional initiatives in development that are intended to strengthen airport security. The first, called SIDA II, is intended to reassess the security of airport secured areas and has been under development for 3 years. The second initiative was the "5-Point Plan" intended to mitigate risks posed by airport workers with enhanced screening measures. However, this initiative was conceived before TSA was directed to implement the worker screening pilot projects, and TSA officials said that the agency is waiting to reassess this effort after the results of the pilot projects are finalized.

Type of security	TSA program/action	Description
	Technology pilot programs	TSA has established two statutorily directed pilot programs to assess airport security technology: • In 2004 TSA initiated the Airport Access Control Pilot Program to test, assess, and provide information on new and emerging technologies. TSA issued a final report on the pilots in December 2006, but officials said that a second round of pilots would be needed for program evaluation. • In 2006 TSA initiated the Airport Perimeter Security pilot project to identify and mitigate existing perimeter security vulnerabilities using commercially available technology. This project was scheduled to conclude in December 2007, and five of the six pilots have been completed.
General airport security	Security directive requirements	TSA uses security directives to impose requirements for strengthening airport security. Since 2004, requirements implemented through security directives were expanded in the area of airport perimeter and access control security. TSA may decide to impose security directive requirements on airport operators through security directives if it determines that such security measures are needed to respond to general or specific threats against the civil aviation system.[a]
	Visible Intermodal Prevention and Response (VIPR) program	Established in December 2005, VIPR uses teams of TSA officials—such as transportation security inspectors, behavior detection officers, bomb appraisal officers, canine handlers, and federal air marshals—and local law enforcement and airport officials to temporarily augment security. VIPR teams perform various functions, including randomly inspecting workers, property, and vehicles, as well as patrolling secure areas across all modes of transportation, including the aviation sector.
	Screening of Passengers by Observation Techniques (SPOT) program	Piloted in 2004 and incrementally expanded as a nationwide program starting in October 2006, SPOT is a screening program in which behavior detection officers use behavior observation and analysis techniques to identify individuals who could pose a security threat.
	Law Enforcement Officer Reimbursement Program[b]	Initiated in April 2002, the Law Enforcement Officer Reimbursement Program was established to provide partial reimbursement for law enforcement presence in support of the passenger screening checkpoint. In June 2003 the program was expanded so officers may also patrol the perimeter, be stationed at access points to assist with worker and passenger screening, or both.

Source: GAO analysis of TSA actions.

[a] Pursuant to 49 C.F.R. part 1542.303, TSA may issue a security directive setting forth requirements when it determines that additional security measures are necessary to respond to a threat assessment or a specific threat against civil aviation. Each airport operator must comply with an applicable security directive within the time prescribed by the security directive.

[b] Pursuant to 49 U.S.C. § 44903(c) and 49 C.F.R. § 1542.215, a commercial airport must maintain a law enforcement presence and capability at the airport in the number and manner adequate to support its security program and other security functions at the airport. According to TSA officials, as part of the Law Enforcement Officer Reimbursement Program, a reimbursable cooperative agreement is negotiated between TSA and the respective airport operator to reimburse the operator for funds expended on law enforcement efforts per the terms of the cooperative agreement. See 49 C.F.R. § 1542.219.

TSA Has Pilot Tested Various Worker Screening Methods, but Significant Program Limitations and Lack of a Sound Evaluation Plan May Limit the Usefulness of the Results

From May through July 2008 TSA piloted a program to screen 100 percent of workers at three airports and to test a variety of enhanced screening methods at four other airports.[64] (See app. V for more detailed information on the pilot program, including locations and types of screening methods used.) According to TSA, the objective of the pilot was to compare 100 percent worker screening and enhanced random worker screening based on (1) screening effectiveness, (2) impact on airport operations, and (3) cost considerations. TSA officials hired a contractor—HSI, a federally funded research and development center—to assist with the design, implementation, and evaluation of the data collected.[65] In July 2009 TSA released a report on the results of the pilot program, which included HSI's findings.[66] HSI concluded that random screening is a more cost-effective approach because it appears "roughly" as effective in identifying contraband items—or items of interest—at less cost than 100 percent worker screening. However, HSI also emphasized that the pilot program "was not a robust experiment" because of limitations in the design and evaluation, such as the limited number of participating airports, which led HSI to identify uncertainties in the results. Given the significance of these limitations, we believe that it is unclear whether random worker screening is more or less cost-effective than 100 percent worker screening.

Specifically, HSI identified what we believe to be significant limitations related to the design of the pilot program and the estimation of costs and operational effects. Limitations related to program design include (1) a limited number of participating airports, (2) the short duration of screening operations (generally 90 days), (3) the variety of screening techniques applied, (4) the lack of a baseline, and (5) limited evaluation of

[64] The Explanatory Statement specifically directed TSA to pilot various methods to screen airport employees (referred to in this report as workers) at a total of seven airports, including 100 percent screening of airport employees at three of the airports for not less than 90 days. At two airports TSA conducted 100 percent worker screening at the passenger screening checkpoint, and one airport conducted 100 percent screening at specifically designated access points in combination with biometric access controls. The enhanced screening methods conducted at four other airports consisted of employee security awareness training, behavioral recognition training, random targeted physical inspections of vehicles and airport workers, new technology, and enhancement of security threat assessment background data checks.

[65] The Secretary of Homeland Security established HSI pursuant to section 312 of the Homeland Security Act of 2002. See 6 U.S.C. § 192.

[66] Transportation Security Administration, *Airport Employee Screening Pilot Program Study: Fiscal Year 2008 Report to Congress.*

enhanced methods.[67] For example, HSI noted that while two of the seven pilot airports performed complete 100 percent worker screening, neither was a Category X airport; a third airport—a Category X—performed 100 percent screening at certain locations for limited durations.[68] HSI also reported that the other four pilot airports used a range of tools and screening techniques—magnetometers,[69] handheld metal detectors, pat-downs—which reduced its ability to assess in great detail any one screening process common to all the pilot airports. In addition, HSI cited issues regarding the use of baseline data for comparison of screening methods. HSI attempted to use previous Aviation Direct Access Screening Program (ADASP) screening data for comparison, but these data were not always comparable in terms of how the screening was conducted. In addition, HSI identified a significant limitation in generalizing pilot program results across airports nationwide, given the limited number and diversity of the pilot airports. HSI noted that because these airports were chosen based on geographic diversity and size, other unique airport factors that might affect worker screening operations—such as workforce size and the number and location of access points—may not have been considered.

HSI also recognized what we believe to be significant limitations in the development of estimates of the costs and operational effects of implementing 100 percent worker screening and random worker screening nationwide.[70] HSI's characterization of its cost estimates as "rough order of magnitude"—or imprecise—underscores the challenge of estimating costs for the entire airport system in the absence of detailed data on individual airports nationwide and in light of the limited amount of information gleaned from the pilot on operational effects and other costs. HSI noted that the cost estimates do not include costs associated with operational effects, such as longer wait times for workers, and potentially costly infrastructure modifications, such as construction of roads and shelters to accommodate vehicle screening. HSI developed high- and low-cost

[67] Transportation Security Administration, *Airport Employee Screening Pilot Program Study: Fiscal Year 2008 Report to Congress.*

[68] This airport did not perform complete 100 percent worker screening because of resource constraints.

[69] A magnetometer is an instrument used to detect prohibited materials.

[70] Transportation Security Administration, *Airport Employee Screening Pilot Program Study: Fiscal Year 2008 Report to Congress.*

estimates based on current and optimal numbers of airport access points and the amount of resources (personnel, space, and equipment) needed to conduct 100 percent and random worker screening. According to these estimates, the direct cost—including personnel, equipment, and other operation needs—of implementing 100 percent worker screening would range from $5.7 billion to $14.9 billion for the first year, while the direct costs of implementing enhanced random worker screening would range from $1.8 billion to $6.6 billion.

HSI noted that the random worker screening methods applied in the worker screening pilot program were a "significant step" beyond TSA's ongoing worker screening program—ADASP—which the agency characterizes as a "random" worker screening program. For the four pilot airports that applied random screening methods, TSA and airport associations agreed to screen a targeted 20 percent of workers who entered secured areas each day.[71] TSA officials also told us that this 20 percent threshold was significantly higher than that applied through ADASP, although officials said that they do not track the percentage of screening events processed through ADASP. TSA officials told us that they do not have sufficient resources to track this information.

In addition to the limitations recognized by HSI, TSA and HSI did not document key aspects of the design and implementation of the pilot program. For example, while they did develop and document a data collection plan that outlined the data requirements, sources, and collection methods to be followed by the seven pilot airports in order to evaluate the program's costs, benefits, and impacts, they did not document a plan for how such data would be analyzed to formulate results. *Standards for Internal Control for the Federal Government* states that significant events are to be clearly documented and the documentation should be readily available for examination to inform management decisions.[72] In addition, in November 2008, based in part on our guide for designing evaluations,[73]

[71] HSI reported that for those airports conducting random worker screening, it was difficult to determine the number of unique individuals screened; for the purposes of the pilot analysis, HSI used the number of screening "events" as a rough proxy for the number of workers screened.

[72] See GAO/AIMD-00-21.3.1. Internal control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results.

[73] GAO, *Designing Evaluations*, GAO/PEMD-10.1.4 (Washington, D.C.: May 1991).

we reported that pilot programs can more effectively inform future program rollout when an evaluation plan is developed to guide consistent implementation of the pilot and analysis of the results.[74] At minimum, a well-developed, sound evaluation plan contains several key elements, including measurable objectives, standards for pilot performance, a clearly articulated methodology, detailed data collection methods, and a detailed data analysis plan.[75] Incorporating these elements can help ensure that the implementation of a pilot generates performance information needed to make effective management decisions. While TSA and HSI completed a data collection plan, and generally defined specific measurable objectives for the pilot program, they did not address other key elements that collectively could have strengthened the effectiveness of the pilot program and the usefulness of the results:

- **Performance standards**. TSA and HSI did not develop and document criteria or standards for determining pilot program performance, which are necessary for determining to what extent the pilot program is effective.

- **Clearly articulated evaluation methodology.** TSA and HSI did not fully articulate and document the methodology for evaluating the pilot program. Such a methodology is to include plans for sound sampling methods, appropriate sample sizes, and comparing the pilot results with ongoing efforts. TSA and HSI documented relevant elements, such as certain sampling methods and sample sizes, in both its overall data collection plan for the program and in individual pilot operations plans for each airport implementing the pilot. However, while officials stated that the seven airports were selected to obtain a range of physical size, worker volume, and geographical dispersion information, they did not document the criteria they used in this process, and could not explain the rationale used to decide which screening methods would be piloted by the individual airports. Because the seven airports tested different screening methods, there were differences in the design of the individual pilots as well as in

[74] GAO-09-45.

[75] Specifically, GAO-09-45 reported that a sound, well-developed and documented evaluation plan includes, at minimum, (1) well-defined, clear, and measurable objectives; (2) criteria or standards for determining pilot program performance; (3) clearly articulated methodology, including sound sampling methods, determination of appropriate sample size for the evaluation design, and a strategy for comparing the pilot results with other efforts; (4) a clear plan that details the type and source of data necessary to evaluate the pilot, methods for data collection, and the timing and frequency of data collection; and (5) a detailed data analysis plan to track the program's performance and evaluate the final results of the project.

the type and frequency of the data collected. While design differences are to be expected given that the pilot program was testing disparate screening methods, there were discrepancies in the plans that limited HSI's ability to compare methods across sites. For example, those airports that tested enhanced screening methods—as opposed to 100 percent worker screening—used different rationales to determine how many inspections would be conducted each day. TSA officials said that this issue and other discrepancies and points of confusion were addressed through oral briefings with the pilot airports, but said that they did not provide additional written instructions to the airports responsible for conducting the pilots. TSA and HSI officials also did not document how they would address deviations from the piloted methods, such as workers who avoided the piloted screening by accessing alternative entry points, or suspension of the pilot because of excessive wait times for workers or passengers (some workers were screened through passenger screening checkpoints). Further, TSA and HSI officials did not develop and document a plan for comparing the results of the piloted worker screening methods with TSA's ongoing random worker screening program to determine whether the piloted methods had a greater impact on reducing insider risk than ongoing screening efforts.

- **Detailed data analysis**. Although the agreement between TSA and HSI also called for the development of a data analysis plan, neither HSI nor TSA developed an analysis plan to describe how the collected data would be used to track the program's performance and evaluate the effectiveness of the piloted screening methods, including 100 percent worker screening. For example, HSI used the number of confiscated items as a means of comparing the relative effectiveness of each screening method.[76] However, HSI reported that the number of items confiscated during pilot operations was "very low" at most pilot airports, and some did not detect any.[77] Based on these data, HSI concluded that random worker screening appeared to be "roughly" as effective in identifying confiscated items as 100 percent worker screening. However, it is possible that there were few or no contraband items to detect, as workers at the pilot airports were warned in advance when the piloted screening methods would be in effect and

[76] HSI defined confiscated items, or "items of interest," as those which TSA did not allow to pass through screening and the possession of which resulted in legal action, disciplinary action, or both against the worker.

[77] HSI reported that seven items of interest were confiscated.

disclosure signs were posted at access points.[78] As a result, comparing the very low rate—and in some cases, nonexistence—of confiscated items across pilots, coupled with the short assessment period, may not fully indicate the effectiveness of different screening methods at different airports. If a data analysis plan had been developed during pilot design, it could have been used to explain how such data would be analyzed, including how HSI's analysis of the pilots' effectiveness accounted for the low confiscation rates.

Because of the significance of the pilot program limitations reported by HSI, as well as the lack of documentation and detailed information regarding the evaluation of the program, the reliability of the resulting data and any subsequent conclusions about the potential impacts, costs, benefits, and effectiveness of 100 percent worker screening and other screening methods cannot be verified. For these reasons, it would not be prudent to base major policy decisions regarding worker screening solely on the results of the pilot program. HSI reported that the wide variation—such as size, traffic flow, and design—of U.S. commercial airports makes it difficult to generalize the seven pilot results to all commercial airports. While we agree it is difficult to generalize the results of such a small sample to an entire population, a well-documented and sound evaluation plan could have helped ensure that the pilot program generated the data and performance information needed to draw reasonable conclusions about the effectiveness of 100 percent worker screening and other methods to inform nationwide implementation. Incorporating these elements into an evaluation plan when designing future pilots could help ensure that TSA's pilots generate the necessary data for making management decisions and that TSA can demonstrate that the results are reliable.

[78] HSI reported that the incident rate—the number of items of interest confiscated compared to the number of workers screened—at both 100 percent and random worker screening airports was less than during the previous 3 months of screening under ADASP, TSA's random screening program.

TSA Has Taken Steps to Strengthen Worker Security Programs, but Issues Remain

Aviation Direct Access Screening Program

According to TSA officials, FSDs and others in the aviation community have long recognized the potential for insiders to do harm from within an airport.[79] TSA officials said that they developed ADASP—a random worker screening program—to counteract the potential vulnerability of airports to an insider attack. According to TSA officials, ADASP serves as an additional layer of security and as a deterrent to workers who seek to smuggle drugs or weapons or to do harm. According to senior TSA officials, FSDs decide when and how to implement ADASP, including the random screening of passengers at the boarding gate or workers at SIDA access points to the sterile area.[80]

TSA officials said that ADASP was initially developed as a pilot project at one airport in March 2005 to deter workers from breaching access controls and procedures for secured areas at that particular airport.[81] According to officials, after concluding that the pilot was successful in deterring airport workers from bringing restricted items into secured areas, TSA began implementing ADASP on a nationwide voluntary basis in August 2006 using existing resources. In March 2007, in response to several incidents of insider criminal activity, TSA directed that ADASP be conducted at all commercial airports nationwide. For example, on March 5, 2007, two airline employees smuggled 14 firearms and 8 pounds of marijuana on

[79] TSA officials said that although FSDs and others had long recognized the threat posed by airport workers, it was considered a “known and accepted risk.” According to these officials, when FSDs raised concerns about the insider threat before 2005, they were told that background checks performed on airport workers were a sufficient safeguard against insider risk.

[80] According to TSA officials, although practices for scheduling ADASP operations vary by airport location, usually FSDs judgmentally schedule them on a staggered and unpredictable basis, varying the time of day, location, and duration. Transportation Security Officers (TSO) typically screen each worker who enters the secured area during these operations, along with property, vehicles, or both, but they may instead decide to screen workers according to a predetermined pattern, such as every second worker. Under TSA procedures, screening locations do not need to cover all access points within an airport, and workers may use alternative entry points to avoid ADASP screenings.

[81] TSA officials also told us that from 2001 through 2006, some airports conducted random worker screening activities similar to ADASP.

board a commercial airplane at Orlando International Airport (based on information received through an anonymous tip, the contraband was confiscated when the plane landed in San Juan, Puerto Rico).

In its October 2008 report, the DHS Office of the Inspector General (OIG) found that ADASP was being implemented in a manner that allowed workers to avoid being screened, and that the program had been applied inconsistently across airports.[82] For example, at most of the seven airports the DHS OIG visited, ADASP screening stations were set up in front of worker access points, which allowed workers to identify that ADASP was being implemented and potentially choose another entry and avoid being screened. However, at another airport, the screening location was set up behind the access point, which prevented workers from avoiding being screened. ADASP standard operating procedures allow ADASP screening locations to be set up in front of or behind direct access points as long as there is signage alerting workers that ADASP screening is taking place. However, the DHS OIG found that the location of the screening stations—either in front of or behind direct access points—affected whether posted signs were visible to workers. The DHS OIG recommended that TSA apply consistent ADASP policies and procedures at all airports, and establish an ADASP working group to consider policy and procedure changes based on an accumulation of best practices across the country. TSA agreed with the DHS OIG's recommendations, and officials stated that they have begun to take action to address them.

Expanded Worker Background Checks

Since April 2004, and in response to our prior recommendation,[83] TSA has taken steps to enhance airport worker background checks. TSA background checks are composed of security threat assessments (STA), which are name-based records checks against various terrorist watch lists, and criminal history record checks (CHRC), which are fingerprint-based criminal records checks. TSA requires airport workers to undergo both

[82] Department of Homeland Security, Office of the Inspector General, *TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening.*

[83] See GAO-04-728. We recommended that TSA determine if and when additional security requirements are needed to reduce the risk posed by airport workers, such as additional background check information.

STAs and CHRCs before being granted unescorted access to secured areas in which they perform their duties.[84]

In July 2004 TSA expanded STA requirements by requiring workers in certain secured areas to submit current biographical information, such as date of birth. TSA further augmented STAs in 2005 to include a citizenship check to identify individuals who may be subject to coercion because of their immigration status or who may otherwise pose a threat to transportation security. In 2007 TSA expanded STA requirements beyond workers with sterile area or SIDA access to apply to all individuals seeking or holding airport-issued identification badges or credentials. Finally, in June 2009 TSA began requiring airport operators to renew all airport identification media every 2 years, deactivate expired media and require workers to resubmit biographical information in the event of certain changes, and expand the STA requirement to include individuals with unescorted access to the AOA, among other things.

TSA has taken steps to strengthen its background check requirements and is considering additional actions to address certain statutory requirements and issues that we identified in 2004.[85] For example, TSA is considering revising its regulation listing the offenses that if a conviction occurred within 10 years of applying for this access, would disqualify a person from receiving unescorted access to secured areas. TSA officials told us that TSA and industry stakeholders are considering whether some disqualifying offenses may warrant a lifelong ban.[86] In addition, while TSA has not yet

[84] In accordance with 49 U.S.C. § 44936, TSA requires airports and air carriers to conduct fingerprint-based records checks for all workers seeking unescorted access to secured areas (which may or may not include the AOA). See 49 C.F.R. §§1542.209, and1544.229. However, TSA requires only STAs for airport workers who apply for unescorted access to an AOA that is not designated as a SIDA.

[85] See GAO-04-728. One issue we raised in 2004 was that of recurrent background checks, and in October 2008, the DHS OIG recommended that TSA mandate recurrent CHRCs and financial records checks for workers with unescorted access to secured areas (see Department of Homeland Security, Office of the Inspector General, *TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening*). TSA stated that it is working on standards for recurrent CHRCs. However, TSA officials said that they do not have evidence that financial problems are a predictor of terrorist activity, so the agency does not plan to require financial records checks.

[86] See 49 C.F.R. § 1542.209(d) (listing 28 offenses that if resulting in a conviction or a verdict of not guilty by reason of insanity within 10 years before the individual applies for unescorted access authority or while the individual has unescorted access authority, would disqualify or revoke that individual's access authority). See also 49 U.S.C. § 44936(b).

specifically addressed a statutory provision requiring TSA to require, by regulation, that individuals with regularly escorted access to secured airport areas undergo background checks,[87] TSA officials told us that they believe the agency's existing measures address the potential risk presented by such workers. They also said that it would be challenging to identify the population of workers who require regularly escorted access because such individuals—for example, construction workers—enter airports on an infrequent and unpredictable basis.

TSA Has Taken Steps to Improve Security Technology, but the Extent to Which TSA Has Addressed Airport Technology Needs Is Unclear

Biometric Access Control Initiatives

Since 2004, TSA has taken some steps to develop biometric worker credentialing;[88] however, it is unclear to what extent TSA plans to address statutory requirements regarding biometric technology, such as developing or requiring biometric access controls at commercial airports in consultation with industry stakeholders.[89] For instance, in October 2008 the DHS OIG reported that TSA planned to mandate phased-in biometric upgrades for all airport access control systems to meet certain

[87] See 49 U.S.C. § 44936(a)(1)(B)(iii).

[88] Biometrics are measurements of an individual's unique characteristics, such as fingerprints, irises, and facial characteristics, used to verify identity.

[89] Among other things, the Intelligence Reform and Terrorism Prevention Act of 2004 directed TSA, in consultation with representatives of the aviation industry, the biometric identifier industry, and the National Institute of Standards and Technology, to establish, at a minimum, (1) comprehensive technical and operational system requirements and performance standards for the use of biometric identifier technology in airport access control systems, (2) a list of products and vendors that meet these requirements, (3) procedures for implementing biometric identifier systems, and (4) best practices for effectively incorporating biometric identifier technology into airport access control systems, including a process to best utilize existing systems and infrastructure. See Pub. L. No. 108-458, § 4011, 118 Stat. 3638, 3712-14 (2004) (codified at 49 U.S.C. § 44903(h)(5)). ATSA also addressed the use of biometric technology to strengthen access control points in secured areas to ensure the security of passengers and aircraft and to consider the deployment of biometric or similar technologies. See 49 U.S.C. § 44903(g)(2)(G), (h)(4)(E).

specifications.[90] However, as of May 2009, according to TSA officials, the agency had not made a final decision on whether to require airports to implement biometric access controls, but it intends to pursue a combination of rule making and other measures to encourage airports to voluntarily implement biometric credentials and control systems.[91] While TSA officials said that the agency issued a security directive in December 2008 that encourages airports to implement biometric access control systems that are aligned with existing federal identification standards,[92] TSA officials also reported the need to ensure that airports incorporate up-to-date standards. These officials also said that TSA is considering establishing minimum requirements to ensure consistency in data collection, card information configuration, and biometric information. Airport operators and industry association officials have called for a consensus-based approach to developing biometric technology standards for airports, and have stressed the need for standards that allow for flexibility and consider the significant investment some airports have already made in biometric technology. Airport operators have also expressed a reluctance to move forward with individual biometric projects because of concerns that their enhancements will not conform to future federal standards.

Although TSA has not decided whether it will mandate biometric credentials and access controls at airports, it has taken steps to assess and develop such technology in response to stakeholder concerns and statutory requirements. For example, TSA officials said the agency has assisted the aviation industry and RTCA, Inc., a federal aviation advisory committee, in developing recommended security standards for biometric access controls, which officials said provide guidelines for acquiring,

[90] Department of Homeland Security, Office of the Inspector General, *TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening*. In this report the DHS OIG recommended that TSA alter regulatory requirements to mandate a phasing in of biometric access controls; according to the report, TSA agreed with this recommendation.

[91] Rule making is a process used by federal agencies to develop, impose, and oversee requirements, and generally affords the regulated entities and other interested parties the opportunity to participate in the process, for example, through public hearings or comment periods. See generally 5 U.S.C. § 553.

[92] The security directive provides that TSA encourages the implementation and use of airport biometric access control systems aligned with Federal Information Processing Standards 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors." (National Institute of Standards and Technology, March 2006.)

designing, and implementing access control systems.[93] TSA officials also noted that the agency has cooperated with the Biometric Airport Security Identification Consortium, or BASIC—a working group of airport operators and aviation association representatives—which has developed guidance on key principles that it believes should be part of any future biometric credential and access control system. In addition, TSA is in the early stages of developing the Aviation Credential Interoperability Solution (ACIS) program.[94] ACIS is conceived as a credentialing system in which airports use biometrics to verify the identities and privileges of workers who have airport- or air carrier–issued identification badges before granting them entry to secured areas. According to TSA, ACIS would provide a trusted biometric credential based on smart card technology (about the size of a credit card, using circuit chips to store and process data) and specific industry standards, and establish standard airport processes for enrollment, card issuance, vetting, and the management of credentials. Although these processes would be standardized nationwide, airports would still be individually responsible for determining access authority. According to TSA officials, the agency is seeking to build ACIS on much of the airports' existing infrastructure and systems and has asked industry stakeholders for input on key considerations, including the population of workers who would receive the credential, program policies, process, technology considerations, operational impacts, and concerns regarding ACIS.

However, as of May 2009, TSA officials could not explain the status of ACIS or provide additional information on the possible implementation of the program since the agency released the specifications for industry comment in April 2008. As a result, it is unclear when and how the agency plans to address the requirements of the Intelligence Reform and

[93] RTCA, Inc., *Integrated Security System Standards for Airport Access Control*, DO 230-B (Washington, D.C., June 19, 2008). These standards provide guidelines for procuring, designing, and implementing access control systems, including testing and evaluating system performance. They also identify, among other things, requirements for physical access controls, video surveillance, security operating centers, intrusion detection, and communications infrastructure. (RTCA, Inc., was formerly known as the Radio Technical Commission for Aeronautics.)

[94] In May 2008, TSA issued ACIS technical specifications to the airport industry, which describe the ACIS system components and requirements, for comment; according to TSA officials, these specifications also discuss many of the technical issues that the agency will consider in establishing standards. As of May 2009, funds had not been appropriated or directed specifically to this initiative, and TSA officials could not provide further information as to the implementation of ACIS.

Terrorism Prevention Act, including establishing minimum standards for biometric systems and determining the best way to incorporate these decisions into airports' existing practices and systems. As of May 2009 TSA officials had not provided any further information, such as scheduled milestones, on TSA's plans to implement biometric technology at airports. Standard practices in program management suggest that developing scheduled milestones can help define the scope of the project, achieve key deliverables, and communicate with key stakeholders.[95] In addition, until TSA communicates its decision on whether it plans to mandate—such as through a rule making—or collaboratively implement biometric access controls at airports, and what approach is best—be it ACIS or another system—operators may be hesitant to upgrade airport security in this area. As we reported in 2004, airport operators do not want to run the risk of installing costly technology that may not comply with future TSA requirements and standards.[96] Developing milestones for implementing a biometric system could help ensure that TSA addresses statutory requirements. In addition, such milestones will provide airports and the aviation industry with the scheduling information needed to plan future security improvements and expenditures.

Technology Pilot Programs

In addition to biometric technology efforts, TSA has also initiated efforts to assess other airport perimeter and access control technology. Pursuant to ATSA, TSA established two pilot programs to assess perimeter and access control security technology, the Airport Access Control Pilot Program (AACPP) in 2004 and the Airport Perimeter Security (APS) pilot program in 2006.[97] AACPP piloted various new and emerging airport security technologies, including biometrics. TSA issued the final report on AACPP in December 2006, but did not recommend any of the piloted technologies for full-scale implementation. TSA officials said that a second round of pilot projects would be necessary to allow time for project evaluation and limited deployments, but as of May 2009 TSA officials said that details for this second round were still being finalized. The purpose of the APS pilot, according to TSA officials, is to identify and mitigate existing airport perimeter security vulnerabilities using commercially

[95] Project Management Institute, *The Standard for Program Management©*, and *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*.

[96] GAO-04-728.

[97] According to TSA officials, the agency established AACPP and APS in response to provisions originally enacted through ATSA. See Pub. L. No.107-71 § 106(d), 115 Stat. at 610 (codified at 49 U.S.C. § 44903(c)(3)).

available technology.[98] APS was originally scheduled to be completed in December 2007, but according to TSA officials, though five of the six pilot projects have been completed, the remaining pilot has been delayed because of problems with the acquisition process. According to TSA officials, the final pilot project is to be completed by October 2009.

TSA officials told us that the agency has also taken steps to provide some technical and financial support to small- and medium-sized airports through AACPP and the APS pilot program, as both tested technologies that could be suitable for airports of these sizes. TSA officials also stated that smaller airports could potentially benefit from the agency's efforts to test the Virtual Perimeter Monitoring System, which was developed by the U.S. Navy and is being installed and evaluated at four small airports. Further, officials noted that TSA has also provided significant funding to support cooperative agreements for the deployment of law enforcement officers at airports—including Category II, III, and IV airports—to help defray security costs. However, according to TSA officials, as of May 2009 TSA had not yet developed a plan, or a time frame for developing a plan, to provide technical information and funding to small- and medium-sized airports, as required by ATSA.[99] According to TSA officials, funds had not been appropriated or specifically directed to develop such a plan, and TSA's resources and management attention have been focused on other statutory requirements for which it has more direct responsibility and deadlines, including passenger and baggage screening requirements. (For a summary of TSA actions to address certain statutory requirements for airport security technology, see app. II.)

[98] The Conference Report accompanying the DHS Appropriations Act, 2006, Pub. L. No. 109-90, 119 Stat. 2064 (2005), allocated $5 million for competitive awards to airports to enhance perimeter security. See H.R. Conf. Rep. No. 109-241, at 54 (2005).

[99] See Pub. L. No. 107-71 § 106(b), 115 Stat. at 609.

TSA Has Taken Action to Improve General Airport Security, but Concerns Exist regarding Implementation of Security Requirements Established by Security Directives

TSA has taken actions to improve general airport security by establishing programs and requirements. For example, TSA has augmented access control screening and general airport security by increasing the presence of transportation security officers and law enforcement officials through the Screening of Passengers by Observation Techniques (SPOT) program and the Law Enforcement Officer Reimbursement Program. In addition, it uses the Visible Intermodal Prevention and Response (VIPR) program, which is used across the transportation sector, to augment airport security efforts. (For more information on these TSA programs, see app. VI.)

TSA uses a variety of regulatory mechanisms for imposing requirements within the transportation sector. In the aviation environment, TSA uses the security directive as one of its regulatory tools for imposing requirements to strengthen the security of civil aviation, including security at the nation's commercial airports.[100] Pursuant to TSA regulation, the agency may decide to use security directives to impose requirements on airport operators if, for example, it determines that additional security measures are needed to respond to general or specific threats against the civil aviation system.[101] As of March 2009 TSA identified 25 security directives or emergency amendments in effect that related to various aspects of airport perimeter and access control security. As shown in table 2, TSA imposed requirements through security directives that address areas such as worker and vehicle screening, criminal history record checks, and law enforcement officer deployments.

Table 2: Requirements Relating to Airport Perimeter and Access Control Security Imposed through Security Directives and Emergency Amendments

	U.S. airports	U.S. air carriers	Foreign air carriers	Total
Number of relevant security directives or emergency amendments	8	7	10	**25**
Areas of regulation addressed				

[100] According to TSA officials, security directives have been the primary means by which the agency imposes security requirements on commercial airports, in addition to measures implemented through the airport operators' TSA-approved security programs. For this reason, we focused our review on requirements related to perimeter and access control security established through security directives. TSA may also impose requirements by amending air carrier security programs and more immediately by issuing emergency amendments to such programs. See, e.g., 49 C.F.R. § 1542.105(d).

[101] See 49 C.F.R. § 1542.303.

	U.S. airports	U.S. air carriers	Foreign air carriers	Total
Access control	6	1	5	**12**
Worker screening	3	3	3	**9**
Vehicle screening	3	0	1	**4**
Criminal history record check	2	1	1	**4**
Security threat assessment	1	2	3	**6**
No-Fly/Selectee lists[a]	3	4	2	**9**
Law enforcement officer deployment	4	0	1	**5**
Airport badging	3	1	3	**7**
Other/miscellaneous	5	2	5	**12**

Source: GAO analysis of TSA security directives and emergency amendments issued to U.S. airport and aircraft operators and foreign air carriers in accordance with 49 C.F.R. parts 1542 (airport security), 1544 (aircraft operator security), and 1546 (foreign air carrier security).

Note: The 25 security directives and emergency amendments may address other areas of security in addition to those related to airport perimeter and access control security.

[a]The No-Fly and Selectee lists contain the names of individuals with known or suspected links to terrorism who may pose a threat to the civil aviation system. In general, passengers identified as a match to the No-Fly list are prohibited from boarding a commercial flight, while those matched to the Selectee list are required to undergo additional screening.

According to TSA officials, security directives enable the agency to respond rapidly to immediate or imminent threats and provide the agency with flexibility in how it imposes requirements on airport operators. This function is especially relevant given the adaptive, dynamic nature of the terrorist threat. Moreover, according to TSA, imposing requirements through security directives is less time consuming than other processes, such as the lengthier notice-and-comment rule making process, which generally provides opportunity for more stakeholder input, requires cost-benefit analysis,[102] and provides the regulated entities with more notice before implementation and enforcement.[103]

Officials from two prominent aviation associations and eight of nine airports we visited identified concerns regarding requirements established through security directive[104]:

- Officials from the two aviation associations noted inconsistencies between requirements established through separate security directives. For example, they noted that the requirements for airport-issued identification badges are different from those for badges issued by an air carrier. Workers employed by the airport, air carrier, or other entities who apply for an airport identification badge granting unescorted access to a secured area are required to undergo an immigration and citizenship status check, whereas workers who apply through an air carrier, which can grant similar unescorted access rights, are not.[105] Both airport and air carrier workers can apply to an airport operator for airport-issued identification badges, but only air carrier workers can apply to their aircraft operator (employer) for an air carrier–issued identification badge. TSA officials told us that the agency plans to address this inconsistency—which has been in effect since December 2002—and is working on a time frame for doing so.

- Airport operator officials from eight of the nine airports we visited and officials from two industry associations expressed concern that requirements established through security directives related to airport

[102] TSA officials told us that although they have not performed cost-benefit analysis when developing perimeter and access control security requirements through security directives, they have considered relevant costs as well as security benefits. However, they could not provide documentation or examples of instances in which they had considered relevant costs as well as security benefits.

[103] Consistent with TSA regulation and as provided for in TSA-issued security directives and emergency amendments, TSA provides regulated entities with an option to request permission to use alternative measures in place of those more specifically imposed by a security directive or emergency amendment. See, e.g., 49 C.F.R § 1542.303(d). For example, from September 2003 through December 2008 TSA received 42 requests for alternatives to requirements imposed through security directives and emergency amendments—TSA officials approved 32 of these requests and denied 9, with 1 remaining pending as of December 2008. (These data do not include the period from August 16, 2006, through September 30, 2006; TSA did not provide data for this period.)

[104] These concerns represent the views of airport operators and industry officials we contacted. We did not independently verify their statements.

[105] This assumes that access privileges for airport and air carrier workers apply to the same or comparable secured areas.

security are often issued for an indefinite time period. Our review of 25 airport security directives and emergency amendments showed that all except one were issued with no expiration date. The two aviation industry associations have expressed concerns directly to TSA that security directive requirements should be temporary and include expiration dates so that they can be periodically reviewed for relevancy.[106]

According to senior officials, TSA does not have internal control procedures for monitoring and coordinating requirements established through security directives related to airport perimeter and access control security. In November 2008 TSA officials told us that the agency had drafted an operations directive that documents procedures for developing, coordinating, issuing, and monitoring civil aviation security directives. According to officials, this operations directive also is to identify procedures for conducting periodic reviews of requirements imposed through security directives. However, while TSA officials told us that they initially planned to issue the operations directive in April 2009, in May 2009 they said that they were in the process of adopting the recommendations of an internal team commissioned to review and identify improvements to TSA's policy review process, including the proposed operations directive. In addition, as of May 2009, officials did not have an expected date for finalizing the directive. TSA officials explained that because the review team's recommendations will require organizational changes and upgrades to TSA's information technology infrastructure, it will take a significant amount of time before an approved directive can be issued. As a result, it is unclear to what extent the operations directive will address concerns expressed by aviation operators and industry stakeholders. Standard practices in program management call for documented milestones to ensure that results are achieved.[107] Establishing milestones for implementing guidance to periodically review airport security requirements imposed through security directives would help TSA formalize review of these directives within a time frame authorized by management.

In addition to the stakeholder issues previously discussed, representatives from two prominent aviation industry associations have expressed concern that TSA has not issued security directives in accordance with the

[106] Our review of the 25 security directives and emergency amendments, however, shows that many of the directives and emergency amendments have been amended one or more times since issuance.

[107] Project Management Institute, *The Standard for Program Management©*.

law. Specifically, these representatives noted that the Transportation Security Oversight Board (TSOB) has not reviewed TSA's airport perimeter and access control security directives in accordance with a provision set forth in ATSA.[108] This provision, as amended, establishes emergency procedures by which TSA may immediately issue a regulation or security directive to protect transportation security, and provides that any such regulation or security directive is subject to review by the TSOB.[109] The provision further states that any regulation or security directive issued pursuant to this authority may remain in effect for a period not to exceed 90 days unless ratified or disapproved by the TSOB. According to TSA officials, the agency has not issued security directives related to airport perimeter and access control security under this emergency authority. Rather, officials explained, the agency has issued such security directives (and all aviation-related security directives) in accordance with its aviation security regulations governing airport and aircraft operators, which predate ATSA and the establishment of TSA.[110] FAA implemented regulations—promulgated through the notice-and-comment rule making process—establishing FAA's authority to issue security directives to impose requirements on U.S. airport and aircraft operators. With the establishment of TSA, FAA's authority to regulate civil aviation security, including its authority to issue security directives,

[108] See Pub. L. No. 107-71, § 101(a), 115 Stat. at 600-01 (codified as amended at 49 U.S.C. § 114(l)).

[109] The TSOB is responsible for, among other things, reviewing and either ratifying or disapproving any regulation or security directive issued by TSA under § 114(l)(2) within 30 days after the date of issuance. See 49 U.S.C. § 115. The TSOB, which is composed of seven cabinet-level members or their designees—the Secretary of Homeland Security (who serves as the chairperson), the Secretary of Transportation, the Attorney General, the Secretary of Defense, the Secretary of the Treasury, the Director of the Central Intelligence Agency, and one member appointed by the President to represent the National Security Council—is to meet at least quarterly, though DHS could not tell us the number of times the TSOB has met since it was established.

[110] See, e.g., 49 C.F.R. §§ 1542.303 (authorizing the issuance of security directives to airport operators) and 1544.305 (authorizing the issuance of security directives to air carriers). FAA possessed and exercised the same authority when it was responsible for aviation security, before the creation of TSA. See 66 Fed. Reg. 37,274 (July 17, 2001) (establishing FAA's authority to issue security directives to airport operators) and 54 Fed. Reg. 28,982 (July 10, 1989) (establishing FAA's authority to issue security directives to aircraft operators). As interpreted by TSA, ATSA intended to give the agency more robust authority to take action in response to emerging threats across all modes of transportation, and in doing so it did not intend to alter (or limit) TSA's existing authority as transferred from FAA.

transferred to the new agency. TSA does not consider ATSA to have altered this existing authority.

A National Strategy for Airport Security Could Help Ensure Program Effectiveness, Inform Cost and Resource Decisions, Ensure Collaboration, and Increase Accountability

Although TSA has developed a variety of individual protective actions to mitigate identified airport security risks, it has not developed a unified national strategy aimed at enhancing airport perimeter and access control security. Through our prior work on national security planning, we have identified characteristics of effective security strategies,[111] several of which are relevant to TSA's numerous efforts to enhance perimeter and access control security. For example, TSA has not developed goals and objectives for related programs and activities, prioritized protective security actions, or developed performance measures to assess the results of its perimeter and access control security efforts beyond tracking outputs (the level of activity provided over a period of time). Further, although TSA has identified some cost information that is used to inform programmatic decision making, it has not fully assessed the costs and resources necessary to implement its airport security efforts. Finally, TSA has not fully outlined how activities are to be coordinated among stakeholders, integrated with other aviation security priorities, or implemented within the agency.[112]

Leading Practices Show That Strategies Help Guide Decision Making and Increase Accountability

Developing a strategy to accomplish goals and desired outcomes helps organizations manage their programs more effectively and is an essential mechanism to guide progress in achieving desired results. Strategies are the starting point and foundation for defining what an agency seeks to accomplish, and we have reported that effective strategies provide an overarching framework for setting and communicating goals and priorities and allocating resources to inform decision making and help ensure accountability.[113] Moreover, a strategy that outlines security goals, as well

[111] See GAO-04-408T, and GAO, *Rebuilding Iraq: More Comprehensive National Strategy Needed to Help Achieve U.S. Goals*, GAO-06-788 (Washington, D.C.: July 11, 2006).

[112] Another recommended characteristic of effective strategies is "risk assessment." However, because we provided details earlier in our report on the steps TSA has taken to assess risks to airport security, we do not discuss risk assessment as a separate characteristic here, rather focusing on risk assessment as one of the many actions that could be aided with the development of an overarching strategy.

[113] GAO, *Agencies' Strategic Plans Under GPRA: Key Questions to Facilitate Congressional Review*, GAO/GGD-10.1.16, Version 1 (Washington, D.C.: May 1997), and GAO-04-408T.

as mechanisms and measures to achieve such goals, and that is understood and available to all relevant stakeholders strengthens implementation of and accountability to common principles.

A national strategy to guide and integrate the nation's airport security activities could strengthen decision making and accountability for several reasons. First, TSA has identified airport perimeter and access control security—particularly the mitigation of risks posed by workers who have unescorted access to secured areas—as a top priority.[114] Historically, TSA has recognized the importance of developing strategies for high-priority security programs involving high levels of perceived risk and resources, such as air cargo security and the SPOT program. Second, in security networks that rely on the cooperation of all security partners—in this case TSA, airport operators, and air carriers—strategies can provide a basis for communication and mutual understanding between security partners that is fundamental for such integrated protective programs and activities. In addition, because of the mutually dependent roles that TSA and its security partners have in airport security operations, TSA's ability to achieve results depends on the ability of all security partners to operate under common procedures and achieve shared security goals. Finally, officials from two prominent industry organizations that represent the majority of the nation's airport operators said that the industry would significantly benefit from a TSA-led strategy that identified long-term goals for airport perimeter and access control security. In addition to providing a unifying framework, a strategy that clearly identifies milestones, developed in cooperation with industry security partners, could make it easier for airport operators to plan, fund, and implement security enhancements that according to industry officials can require intensive capital improvements.

While TSA has taken steps to assess threat and vulnerability related to airport security and developed a variety of protective actions to mitigate risk, TSA has not developed a unifying strategy to guide the development,

[114] For each transportation mode TSA has identified areas it plans to target for reducing risk to the maximum extent possible. TSA's fiscal year 2009 focus for commercial airports is high-risk airports and airport workers. It is not clear, however, what actions TSA has taken, or plans to take, to achieve this reduction in risk. As of March 2009 TSA had not provided documentation on the details of its plans. We have previously reported that TSA's approach to identifying high-risk focus areas is not based on criteria established in the NIPP, and recommended that TSA work with DHS to validate its risk management approach by establishing a plan and time frame for assessing the appropriateness of its approach (see GAO-09-492).

implementation, and assessment of these varied actions and those of its security partners. TSA officials cited three reasons why the agency has not developed a strategy to guide national efforts to enhance airport security. First, TSA officials cited a lack of congressional emphasis on airport perimeter and access control security relative to other high-risk areas, such as passenger and baggage screening. Second, these officials noted that airport operators, not TSA, have operational responsibility for airport security. Third, they cited a lack of resources and funding.

While these issues may present challenges, they should be considered in light of other factors. First, Congress has long recognized the importance of airport security, and has contributed to the establishment of a variety of requirements pertaining to this issue.[115] For example, the appropriations committees, through reports accompanying DHS's annual appropriations acts, have directed TSA to focus its efforts on enhancing several aspects of airport perimeter and access control security.[116] Moreover, developing a strategy that clearly articulates the risk to airport security and demonstrates how those risks can be addressed through protective actions could help inform decision making. Second, though we recognize that airport operators, not TSA, generally have operational responsibility for airport perimeter and access control security, TSA—as the regulatory authority for airport security and the designated lead agency for transportation security—is responsible for identifying, prioritizing, and coordinating protection efforts within aviation, including those related to airport security. TSA currently exercises this authority by ensuring compliance with TSA-approved airport operator security programs and, pursuant to them, by issuing and ensuring compliance with requirements imposed through security directives or other means. Finally, regarding resource and funding constraints, federal guidelines for strategies and planning include linking program activities and anticipated outcomes with

[115] For example, ATSA contained a variety of provisions addressing risks posed by airport workers, such as amending requirements related to TSA background checks of workers with access to secured areas, mandating that TSA establish a pilot program to test and evaluate access control protections for secured areas, and establishing an ongoing requirement that TSA assess and test airport operator compliance with access control requirements and report annually on its findings. See, e.g., 49 U.S.C. §§ 44903(c)(3), (g)(2)(D), 44936(a)(1)(B)(iii), (a)(1)(C)(i). App. II provides a list of related ATSA provisions and TSA's efforts to address these requirements.

[116] For example, of amounts appropriated to TSA through Division E of the Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, Div. E, 121 Stat. 1844, 2042 (2007), the accompanying Explanatory Statement directed $37 million of its appropriation for, among other things, airport worker screening.

expected program costs.[117] In this regard, a strategy could strengthen decision making to help allocate limited resources to mitigate risk, which is a cornerstone of homeland security policy. Additionally, DHS's risk management approach recognizes that resources are to be focused on the greatest risks, and on protective activities designed to achieve the biggest reduction in those risks given the limited resources at hand. The NIPP risk management framework provides guidance for agencies to develop strategies and prioritize activities to those ends.

A strategy helps to link individual programs to specific performance goals and describe how the programs will contribute to the achievement of those goals. A national strategy could help TSA, airport operators, and industry stakeholders in aligning their activities, processes, and resources to support mission-related outcomes for airport perimeter and access control security, and, as a result, in determining whether their efforts are effective in meeting their goals for airport security.

TSA Has Not Identified Security Goals or Priorities or Fully Assessed the Effectiveness of Its Actions to Strengthen Airport Security

Our previous work has identified that an essential characteristic of effective strategies is the setting of goals, priorities, and performance measures. This characteristic addresses what a strategy is trying to achieve and the steps needed to achieve and measure those results. A strategy can provide a description of an ideal overall outcome, or "end-state," and link individual programs and activities to specific performance goals, describing how they will contribute to the achievement of the end-state. The prioritization of programs and activities, and the identification of milestones and performance measures, can aid implementing parties in achieving results according to specific time frames, as well as enable effective oversight and accountability. The NIPP also calls for the development of goals, priorities, and performance measures to guide DHS components, including TSA, in achieving a desired end-state.

Goals

Security goals allow stakeholders to identify the desired outcomes that a security program intends to achieve and that all security partners are to work to attain. Defining goals and desired outcomes, in turn, enables stakeholders to better guide their decision making to develop protective security programs and activities that mitigate risks. The NIPP also states

[117] Office of Management and Budget Circular No. A-11, Part 6, *Preparation and Submission of Strategic Plans, Annual Performance Plans, and Annual Program Performance Reports* (June 2005).

that security goals should be used in the development of specific protective programs and considered for distinct assets and systems. However, according to TSA officials, the agency has not developed goals and objectives for airport security, including specific targets or measures related to the effectiveness of security programs and activities.[118] TSA officials told us that the agency sets goals for aviation security as a whole but has not set goals and objectives for the airport perimeter and access control security area. Developing a baseline set of security goals and objectives that consider, if not reflect, the airport perimeter and access control security environment would help provide TSA and its security partners with the fundamental tools needed to define outcomes for airport perimeter and access control security. Furthermore, a defined outcome that all security partners can work toward will better position TSA to provide reasonable assurance that it is taking the most appropriate steps for ensuring airport security.

Priorities

Our past work has also shown that the identification of program priorities in a strategy aids implementing parties in achieving results, which enables more effective oversight and accountability. Although TSA has implemented protective programs and activities that address risks to airport security, according to TSA officials it has not prioritized these activities nor has it yet aligned them with specific goals and objectives. TSA officials told us that in keeping with legislative mandates, they have focused agency resources on aviation security programs and activities that were of higher priority, such as passenger and baggage screening and air cargo security. Identifying priorities related to airport perimeter and access control security could assist TSA in achieving results within specified time frames and limited resources because it would allow the agency to concentrate on areas of greatest importance.

Performance Measures

In addition to our past work on national strategies, the NIPP and other federal guidance require agencies to assess whether their efforts are effective in achieving key security goals and objectives so as to help drive future investment and resource decisions and adapt and adjust protective

[118] TSA has documented, measurable goals for two specific activities—compliance inspections (95 percent compliance rate for airports with respect to leading security indicators) and security threat assessments (100 percent assessment of workers who have airport-issued badges).

efforts as risks change.[119] Decision makers use performance measurement information, including activity outputs and descriptive information regarding program operations, to identify problems or weaknesses in individual programs, identify factors causing the problems, and modify services or processes to try to address problems.[120] Decision makers can also use performance information collectively, and, according to the NIPP, examine a variety of data to provide a holistic picture of the health and effectiveness of a security approach from which to make security improvements.[121] If significant limitations on performance measures exist, the strategy might address plans to obtain better data or measurements, such as national standards or indicators of preparedness.

TSA officials told us that TSA has not fully assessed the effectiveness of its protective activities for airport perimeters and secured areas, but they said that the agency has taken some steps to collect certain performance data for some airport security programs and activities to help inform programmatic decision making. For example, TSA officials told us that they require protective programs, such as ADASP and VIPR, to report certain output data and descriptive program information, which officials use to inform administrative or programmatic decisions. For ADASP, TSA requires FSDs to collect information on, among other things, the number of workers screened, vehicles inspected, and prohibited items surrendered. TSA officials said that they use these descriptive and output data to inform programmatic decisions, such as determining the number of staff days needed to support ADASP operations nationwide. However, TSA was not able to provide documentation on how such analysis has been

[119] Internal control standards and the Government Performance and Results Act of 1993 also call for agencies to have measures and indicators linked to mission, goals, and objectives to allow for comparisons to be made among different sets of data (for example, desired performance against actual performance), so that corrective actions can be taken if necessary. See, generally, GAO/AIMD-00-21.3.1, Pub. L. No. 103-62, 107 Stat. 285 (1993); and Office of Management and Budget Circular No. A-11, Part 6, *Preparation and Submission of Strategic Plans, Annual Performance Plans, and Annual Program Performance Reports* (Washington, D.C.: June 2005).

[120] Performance measurement is the ongoing monitoring and reporting of program accomplishments and progress toward preestablished goals.

[121] According to the NIPP, there are three types of performance measures: *descriptive measures*, which generally describe sector resources and activities, but do not reflect performance; *output measures*, which are used to measure whether specific activities are performed as planned, track the progression of a task, or report on the output of a process; and *outcome measures*, which track progress toward an intended goal by beneficial results rather than level of activity.

conducted. For VIPR, officials said that they require team members to complete after-action reports that include data on the number of participants, locations, and types of activities conducted. TSA officials said that they are analyzing and categorizing this descriptive and output information to determine trends and identify areas of success and failure, which they will use to improve future operations, though they did not provide us with examples of how they have done this. TSA officials also told us that they require SPOT to report descriptive operations data and situational report information, which are to be used to assign necessary duties and correct problems with program implementation. However, TSA officials could not tell us how they use these descriptive and output data to inform program development and administrative decisions. While the use of descriptive and output data to inform program development and administration is both appropriate and valuable, leading management practices emphasize that successful performance measurement focuses on assessing the results of individual programs and activities.[122]

TSA officials also told us that while they recognize the importance of assessing the effectiveness of airport security programs and activities in reducing known threats, it is difficult to do so because the primary purpose of these activities is deterrence. Assessing the deterrent benefits of a program is inherently challenging because it involves determining what would have happened in the absence of an intervention, or protective action, and it is often difficult to isolate the impact of the individual program on behavior that may be affected by multiple other factors. Because of this difficulty, officials told us that they have instead focused their efforts on assessing the extent to which each airport security activity supports TSA's overall layered approach to security. We recognize that assessing the effectiveness of deterrence-related activities is challenging and that it continues to be the focus of ongoing analytic effort and policy review. For example, a January 2007 report by the Department of Transportation addressed issues related to measuring deterrence in the maritime sector,[123] and a February 2007 report by the RAND Corporation acknowledged the challenges associated with measuring the benefits of

[122] See S. Rep. No. 103-58 (1993) (accompanying the Government Performance and Results Act).

[123] The Department of Transportation, *Assessment of Performance Measures for Security of Maritime Transportation Network, Port Security Metrics: Proposed Measurement of Deterrence Capability* (Washington, D.C., January 2007).

security programs aimed at reducing terrorist risk.[124] However, as a feature of TSA's layered security approach, many of its airport activities address other aspects of security in addition to deterrence. Like other homeland security efforts, TSA's airport security activities also seek to limit the potential for attack, safeguard critical infrastructure and property, identify wrongdoing, and ensure an effective and efficient response in the event of an attack; the desired outcome of its efforts is to reduce the risk of an attack. Deterrence is an inherent benefit of any protective action, and methods designed to detect wrongdoing and measures taken to safeguard critical infrastructure and property, for example, also help deter terrorist attacks. There are a number of activities that TSA has implemented that seek to reduce this risk, such as requiring security threat assessments for all airport workers. Some of these activities serve principally to deter, such as ADASP, while others are more focused on safeguarding critical infrastructure and property, such as conducting compliance inspections of aviation security regulations or installing perimeter fencing. Some activities serve multiple purposes, such as VIPR, which seeks to provide a visual deterrent to terrorist or other criminal activity, but also seeks to safeguard critical infrastructure in various modes of transportation. Examining the extent to which its activities have effectively addressed these various purposes would enable TSA to more efficiently implement and manage its programs.

There are several methods available that TSA could explore to gain insight on the extent to which its security activities have met their desired purpose and to ultimately improve program performance. For example, TSA could work with stakeholders, such as airport operators and other security partners, to identify and share lessons learned and best practices across airports to better tailor its efforts and resources and continuously improve security. TSA could also use information gathered through covert testing or compliance inspections—such as noncompliance or security breaches—to make adjustments to specific security activities and to identify which aspects require additional investigation. In addition, TSA could develop proxy measures—indirect measures or signs that approximate or represent the direct measure—to show how security efforts correlate to an improved security outcome. Appendix VII provides

[124] Brian A. Jackson, *Assessing the Benefits of Homeland Security Efforts Deployed Against a Dynamic Terrorist Threat* (Santa Monica, Calif.: Rand Corporation, February 2007).

a complete discussion on these methods, as well as information on other alternatives TSA could explore.

TSA Has Identified Costs for Some Airport Security Activities, but Has Not Fully Identified Costs and Resource Needs, and Has Generally Not Conducted Cost-Benefit Analysis to Prioritize and Allocate Resources for Airport Security Activities

Our prior work shows that effective strategies address costs, resources, and resource allocation issues. Specifically, effective strategies address the costs of implementing the individual components of the strategy, the sources and types of resources needed (such as human capital or research and development), and where those resources should be targeted to better balance risk reductions with costs.[125] Effective strategies may also address in greater detail how risk management will aid implementing parties in prioritizing and allocating resources based on expected benefits and costs. Our prior work found that strategies that provide guidance on costs and needed resources help implementing parties better allocate resources according to priorities, track costs and performance, and shift resources as appropriate.

Costs and Resources

Statutory requirements and federal cost accounting standards also stress the benefits of developing and reporting on the cost of federal programs and activities, as well as using that information to more effectively allocate resources and inform program management decisions.[126] TSA has identified the costs and resources it needs for some specific activities and programs that exclusively support airport security, such as JVAs of selected commercial airports. However, for programs that serve airport security as well as other aspects of aviation security, TSA has not identified the costs and resources devoted to airport security. For example, TSA has identified its expenditures for compliance inspections and other airport security–related programs and activities, which collectively totaled nearly $850 million from fiscal years 2004 through 2008. However, TSA has not identified what portion of these funds was directly allocated for airport security activities versus other aviation security activities, such as passenger screening. (For a more detailed discussion of airport security costs, see app. IV.) Further, TSA has not fully identified the resources it needs to mitigate risks to airport perimeter and

[125] GAO-04-408T.

[126] See Chief Financial Officers Act of 1990, Pub. L. No. 101-576, 104 Stat. 2838 (1990); The Statement of Federal Financial Accounting Standards No. 4, *Managerial Cost Accounting Concepts and Standards for the Federal Government*; the Joint Financial Management Improvement Program, *Framework for Federal Financial Management Systems*; and the Federal Financial Management Improvement Act of 1996, Pub. L. No. 104-208, Div. A., tit. VIII, 110 Stat. 3009, 3009-389 (1996).

access control security. According to TSA officials, identifying collective agency costs and resource needs for airport security activities is challenging because airport security is not a separately funded TSA program, and many airport security activities are part of broader security programs. However, without attempting to identify total agency costs, it will be difficult for TSA to identify costs associated with individual security activities, and therefore it will be hindered in determining the resources it needs to sustain desired activity levels and realize targeted results. While TSA officials told us that they are starting to identify costs for airport security activities and plan to complete this effort by the end of 2009, they could provide no additional information to illustrate their approach for doing so. As a result, it is unclear what costs the agency will identify, and to what extent TSA will be able to identify costs for specific security activities in order to identify the resources it needs to sustain desired activity levels and realize targeted results.

TSA officials also told us that they have not yet identified or estimated costs to the aviation industry for implementing airport security requirements, such as background checks for their workers, or capital costs—such as construction and equipment—that airport operators incur to enhance the security of their facilities.[127] According to these officials, the agency does not have the resources and funds to collect cost information from airport operators. However, TSA officials could not tell us how and to what extent they had assessed the resources and funds needed to collect this information or whether they had explored other options for collecting cost data, such as working with industry associations to survey airport operators. Estimating general cost information on the types and levels of resources needed for desired outcomes would provide TSA and other stakeholders with valuable information with which to make informed resource and investment decisions, including decisions about future allocation needs, to mitigate risks to airport security.

Prioritizing and Allocating Resources

According to our previous work on effective national strategies, as well as NIPP guidance, risk management focuses security efforts on those activities that bring about the greatest reduction in risk given the resources used.[128] According to federal guidance, employing systematic cost-benefit analysis helps ensure that agencies choose the security

[127] In November 2008 TSA officials stated that the agency plans to hire a contractor in 2009 to develop relevant cost data for the background checks program.

[128] GAO-04-408T.

priorities that most efficiently and effectively mitigate risk for the resources available. The Office of Management and Budget (OMB) cites cost-benefit analysis as one of the key principles to be considered when an agency allocates resources for capital expenditures because it provides decision makers with a clear indication of the most efficient alternative.[129] DHS's Cost-Benefit Analysis Guidebook also states that cost-benefit analysis identifies the superior financial solution among competing alternatives, and that it is a proven management tool to support planning and managing costs and risks.[130] While TSA has made efforts to consider costs for some airport security programs, it has not used cost-benefit analysis to allocate or prioritize resources toward the most cost-effective alternative actions for mitigating risk.[131]

According to TSA officials, certain factors have limited TSA's ability to conduct cost-benefit analysis, such as resource constraints and the need to take immediate action to address new and emerging security threats. However, officials could not demonstrate that they had attempted to conduct cost-benefit analysis for programs and activities related to airport security within the constraints of current resources, or explain how, or to what extent, they had assessed the resources that would be needed to conduct cost-benefit analysis. Further, TSA officials could not cite a situation in which the need to take immediate action—outside of issuing

[129] See OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget* (July 2007); OMB Circular No. A-94, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*; and OMB Circular No. A-4, *Regulatory Analysis* (September 2003). According to federal guidance, cost-benefit analysis is a systematic method for assessing the desirability of alternative projects or policies by combining estimated costs with benefits. The goal of cost-benefit analysis is to promote efficient resource allocation through well-informed decision making, and it is considered a proven management tool that assists in planning a project and managing costs and risks.

[130] Department of Homeland Security, *Cost-Benefit Analysis Guidebook*, Version 2.0 (Washington, D.C., February 2006).

[131] In 2007, TSA worked with the United States Commercial Aviation Partnership to evaluate the cost and operational impacts of several proposed worker screening alternatives, including 100 percent worker screening. However, this evaluation focused solely upon the economic and operational impacts of these alternatives and did not evaluate benefits to security. TSA has also conducted a congressionally directed pilot program to help better identify the potential costs and benefits of 100 percent worker screening as an alternative to random worker screening. Based on the results of this pilot program, TSA concluded that random screening is a more cost-effective approach than 100 percent worker screening because it appeared "roughly" as effective in identifying contraband items at less cost. However, because of the significant limitations related to the design and evaluation of the pilot program, we believe that it is unclear based on the program results whether random worker screening is more or less cost-effective than 100 percent worker screening.

security directives—in response to a threat prevented them from conducting cost-benefit analysis.[132] TSA officials agreed that conducting cost-benefit analysis is beneficial, but also said that it is not always practical because of the difficulty in quantifying the benefits of deterrence-based activities. Because of this challenge, officials said that they have used professional judgment, past experience, law enforcement principles, and intelligence information to evaluate alternative airport security activities to mitigate risks.[133] While TSA's approach to identifying security actions includes accepted risk reduction decision-making tools, such as professional judgment, it does not provide a means to fully weigh the benefits versus the costs of implementing alternative actions. However, despite the challenges TSA cited to developing cost-benefit analysis, TSA officials told us that as of January 2009, the agency was in the early stages of investigating costs and benefits related to airport perimeter access control. According to these officials, TSA plans to initially focus on developing cost estimates associated with improving access control, a process the agency expects to complete by the end of 2009. However, because TSA officials did not explain how they expect to identify and estimate these costs and how, in the future, they plan to identify and estimate benefits for alternative actions, especially those actions that focus on deterrence, it is not yet clear to what extent TSA's efforts will constitute cost-benefit analysis.

The use of systematic cost-benefit analysis when considering future airport security measures would help TSA to choose the most cost-effective security options for mitigating risk. We recognize the difficulties in quantifying the benefits of deterrence-based activities, but there are alternatives that TSA could pursue to assess benefits, such as examining the extent to which its activities address other purposes besides

[132] According to TSA officials, in the event of an immediate or imminent threat the agency uses security directives to impose requirements on airport operators, which does not require TSA to conduct cost-benefit analysis. However, officials told us that even in these circumstances they have considered relevant costs as well as benefits to proposed requirements, although they could not provide documentation or relevant examples.

[133] For example, TSA officials said that they used professional judgment to determine that ADASP was the most appropriate security action to mitigate the insider risk, and did not study alternatives to random screening, such as 100 percent worker screening, or assess whether random screening was the most cost-effective option. Officials said that at the time they developed ADASP, staffing and budget options made 100 percent worker screening an unrealistic option. TSA officials also said that they used a similar approach to develop SPOT, in that they did not use cost-benefit analysis to compare the advantages and costs of other alternative programs.

deterrence. Moreover, OMB recognizes that in some circumstances—such as when data are insufficient—costs and benefits cannot be quantified, in which case costs and benefits are to be assessed in qualitative terms.[134] By exploring ways to identify expected costs associated with alternatives, and balancing these with estimated security benefits, TSA can more fully ensure that it is efficiently allocating and prioritizing its limited resources, as well as those of individual airports, in a way that maximizes the effectiveness of its airport security efforts.

TSA Has Collaborated with Stakeholders regarding Airport Security Activities, but Has Not Always Fully Coordinated or Integrated Airport Security with Other Aspects of Aviation Security

Our prior work shows that effective national strategies address how to coordinate efforts and resolve conflicts among stakeholders, address ways in which each strategy relates to the goals of other strategies, and devise plans for implementing the strategies.[135] Because the responsibility for airport perimeter and access control security involves multiple stakeholders, including federal entities, individual airport operators, air carriers, and industry organizations, coordination among stakeholders is critical. In such an environment, the implementation of security activities is strengthened when a strategy addresses how federal efforts will coordinate and integrate with other federal and private sector initiatives, relate to the goals and objectives of other strategies and plans, and be implemented and coordinated by relevant parties.

Coordination

Representatives from industry associations told us that while TSA has collaborated with industry stakeholders on the development of multiple airport security activities and initiatives, the agency has not always fully coordinated the development and implementation of specific security activities and initiatives. For example, although TSA has worked with the industry in the development of some aspects of airport security technology, such as biometrics, industry association officials told us that the agency has not yet recommended specific technology based on the results of technology-based pilot programs it completed over 2 years ago in 2007. These officials also noted that TSA did not fully coordinate with the industry in its decision to impose stronger requirements on worker credentialing practices in the wake of security incidents at individual airports. TSA officials said that they have worked closely with industry stakeholders in addressing airport security issues, and have established

[134] See OMB Circular No. A-4. Examples of qualitative measures cited by OMB include the costs and benefits of privacy protection.

[135] GAO-04-408T.

working groups to continue to coordinate on issues such as biometric access control security. Our prior work found that a strategy should provide both direction and guidance to government and private entities so that missions and contributions can be more appropriately coordinated.[136]

Integration and Implementation

TSA has not demonstrated how it relates the activities of airport security to the goals, objectives, and activities of TSA's other aviation security strategies, such as passenger screening, air cargo screening, and baggage screening. In addition, TSA has not identified how these various security areas are coordinated at the national level. For example, TSA officials told us that some security efforts, such as the random worker screening program and roving security response teams,[137] are used to address multiple security needs, such as both passenger and worker screening, but could not identify the extent to which program resources are planned for and applied between competing security needs. TSA officials said that decisions to allocate random worker screening resources between passenger and worker screening are made at the local airport level by FSDs. However, a clear understanding of how TSA's needs and goals for airport security align with those of its other security responsibilities would enable the agency to better coordinate its programs, gauge the effectiveness of its actions, and allocate resources to its highest-priority needs. Finally, it is not clear to what extent TSA has coordinated airport security activities within the agency, the responsibilities for which are spread among multiple offices. TSA officials explained that agency efforts to enhance and oversee airport perimeter and access control security are spread across multiple programs within five TSA component offices. No one office or program has responsibility for coordinating and integrating actions that affect the numerous aspects of perimeter and access control security, including operations, technology, intelligence, program policy, credentialing, and threat assessments. TSA officials agreed that the diffusion of responsibilities across offices can present coordination challenges. Developing an overarching, integrated framework for coordinating actions between implementing parties could better position TSA to avoid unnecessary duplication, overlap, and conflict in the implementation of these actions. According to our past work, strategies that provide guidance to clarify and link the roles, responsibilities, and capabilities of the implementing parties can foster more effective implementation and accountability.

[136] GAO-04-408T.

[137] These programs—ADASP and VIPR—are discussed in more detail later in this report.

Conclusions

Commercial airports facilitate the movement of millions of passengers and tons of goods each week and are an essential link in the nation's transportation network. Given TSA's position that the interconnected commercial airport network is only as strong as its weakest asset, determining vulnerability across this network is fundamental to determining the actions and resources that are necessary to reasonably protect it. Evaluating whether existing, select vulnerability assessments reflect the network of airports will help TSA ensure that its actions strengthen the whole airport system. If TSA finds that additional assessments are needed to identify the extent of vulnerabilities nationwide, then developing a plan with milestones for conducting those assessments, and leveraging existing available assessment information from stakeholders, would help ensure the completion of these assessments and that intended results are achieved. In addition, although the consequences of a successful terrorist breach in airport security have not been assessed, based on the past events, the potential impact on U.S. assets, safety, and public morale could be profound. For this reason, assessing the likely consequences of an attack is an essential step in assessing risks to the nation's airports. Further, a comprehensive risk assessment that combines threat, vulnerability, and consequence would help TSA determine which risks should be addressed—and to what degree—and would help guide the agency in identifying the necessary resources for addressing these risks. Moreover, documenting milestones for completing the risk assessment would help ensure its timely completion.

Implementing and evaluating a pilot program can be challenging, especially given the individual characteristics of the sites involved in the worker screening pilot, such as the variation in airport size, traffic flows, and layouts. However, a well-developed and documented evaluation plan, with well-defined and measurable objectives and standards as well as a clearly articulated methodology and data analysis plan, can help ensure that a pilot program is implemented and evaluated in ways that generate reliable information to inform future program development decisions. By making such a plan a cornerstone of future pilot programs, TSA will be better able to ensure that the results of those pilot programs will produce the reliable data necessary for making the best program and policy decisions.

Integrating biometric technology into existing airport access control systems will not be easy given the range of technologies available, the number of stakeholders involved, and potential differences in the biometric controls already in use at airports. Yet Congress, the administration, and the aviation industry have emphasized the need to move forward in implementing such technology to better control access to sensitive airport areas. But until TSA decides whether, when, and how it will mandate biometric access controls at airports, individual airport operators will likely continue to delay investing in potentially costly technology in case it does not comply with future federal standards. Establishing milestones for addressing requirements would not only provide airports with the necessary information to appropriately plan future security upgrades, but give all stakeholders a road map by which they can anticipate future developments.

TSA uses security directives as a means for establishing additional security measures in response to general or specific threats against the civil aviation system, including the security of airport perimeters and the controls that limit access to secured airport areas. Just as it is important that federal agencies have flexible mechanisms for responding to the adaptive, dynamic nature of the terrorist threat, it is also important that requirements remain consistent with current threat information. Establishing milestones for periodically reviewing airport perimeter and access control requirements imposed through security directives would help provide TSA and stakeholders with reasonable assurance that TSA's personnel will review these directives within a time frame authorized by management.

TSA, along with industry partners, has taken a variety of steps to implement protective measures to strengthen airport security, and many of these efforts have required numerous stakeholders to implement a range of activities to achieve desired results. These various actions, however, have not been fully integrated and unified toward achieving common outcomes and effectively using resources. A national risk-informed strategy—that establishes measurable goals, priorities, and performance measures; identifies needed resources; and is aligned and integrated with related security efforts—would help guide decision making and hold all public and private security partners accountable for achieving key shared outcomes within available resources. Moreover, a strategy that identifies these key elements would allow TSA to better articulate its needs—and the challenge of meeting those needs—to industry stakeholders and to Congress. Furthermore, balancing estimated costs against expected security benefits, and developing measures to assess the effectiveness of security activities, would help TSA provide reasonable assurance that it is properly allocating and prioritizing its limited resources, or those of airports, in a way that maximizes the effectiveness of its airport security efforts.

Recommendations for Executive Action

To help ensure that TSA's actions in enhancing airport security are guided by a systematic risk management approach that appropriately assesses risk and evaluates alternatives, and that it takes a more strategic role in ensuring that government and stakeholder actions and resources are effectively and efficiently applied across the nationwide network of airports, we recommend that the Assistant Secretary of TSA work with aviation stakeholders to implement the following five actions:

- Develop a comprehensive risk assessment for airport perimeter and access control security, along with milestones (i.e., time frames) for completing the assessment, that (1) uses existing threat and vulnerability assessment activities, (2) includes consequence analysis, and (3) integrates all three elements of risk—threat, vulnerability, and consequence.
    - As part of this effort, evaluate whether the current approach to conducting JVAs appropriately and reasonably assesses systems vulnerabilities, and whether an assessment of security vulnerabilities at airports nationwide should be conducted.
    - If the evaluation demonstrates that a nationwide assessment should be conducted, develop a plan that includes milestones for completing the nationwide assessment. As part of this effort, leverage existing assessment information from industry stakeholders, to the extent feasible and appropriate, to inform its assessment.
- Ensure that future airport security pilot program evaluation and implementation efforts include a well-developed and well-documented evaluation plan that includes
    - measurable objectives,
    - criteria or standards for determining program performance,
    - a clearly articulated methodology,
    - a detailed data collection plan, and
    - a detailed data analysis plan.
- Develop milestones for meeting statutory requirements, in consultation with appropriate aviation industry stakeholders, for establishing system requirements and performance standards for the use of biometric airport access control systems.
- Develop milestones for establishing agency procedures for reviewing airport perimeter and access control requirements imposed through security directives.

- To better ensure a unified approach among airport security stakeholders for developing, implementing, and assessing actions for securing airport perimeters and access to controlled areas, develop a national strategy for airport security that incorporates key characteristics of effective security strategies, including the following:
    - Measurable goals, priorities, and performance measures. TSA should also consider using information from other methods, such as covert testing and proxy measures, to gauge progress toward achieving goals.
    - Program cost information and the sources and types of resources needed. TSA should also identify where those resources would be most effectively applied by exploring ways to develop and implement cost-benefit analysis to identify the most cost-effective alternatives for reducing risk.
    - Plans for coordinating activities among stakeholders, integrating airport security goals and activities with those of other aviation security priorities, and implementing security activities within the agency.

Agency Comments and Our Evaluation

We provided a draft of our report to DHS and TSA on August 3, 2009, for review and comment. On September 24, 2009, DHS provided written comments, which are reprinted in appendix VIII. In commenting on our report, DHS stated that it concurred with all five recommendations and identified actions planned or under way to implement them.

In its comments to our draft report, DHS stated that the Highlights page of our report includes a statement that is inaccurate. We disagree. Specifically, DHS contends that it is not accurate to state that TSA "has not conducted vulnerability assessments for 87 percent of the nation's 450 commercial airports" because this statement does not recognize that TSA uses other activities to assess airport vulnerabilities, and that these activities are conducted for every commercial airport. For example, DHS stated that (1) every commercial airport must have a TSA-approved ASP, which is to cover personnel, physical, and operational security measures; (2) each ASP is reviewed on a regular basis by a FSD; and (3) such FSD reviews "include a review of security measures applied at the perimeter." As we noted in our report, TSA identified JVAs, along with professional judgment, as the agency's primary mechanism for assessing airport security vulnerabilities in accordance with NIPP requirements. Moreover, it is not clear to what extent the FSD reviews and other activities TSA cites in its comments address airport perimeter and access control vulnerabilities or to what extent such reviews have been applied consistently on a nationwide basis, since TSA has not provided us with any documentary evidence regarding these or other reviews. Finally, in meeting with TSA, its officials acknowledged that because they have not conducted a joint vulnerability assessment for 87 percent of commercial airports, they do not know how vulnerable these airports are to an intentional breach in security or an attack. Thus, we consider the statement on our Highlights page to be accurate.

TSA also stated that “as provided in our draft report” the foundation of TSA’s national strategy is its individual layers—or actions—of security, which, when combined, generate an exponential increase in deterrence and detection capability. However, we did not evaluate TSA’s layered approach to security or the extent to which this approach provides increased deterrence and detection capabilities.

Regarding our first recommendation that TSA develop a comprehensive risk assessment for airport perimeter and access control security, DHS stated that TSA will develop such an assessment through its ongoing efforts to conduct a comprehensive risk assessment for the transportation sector. TSA intends to provide the results of the assessment to Congress by January 2010. According to DHS, the aviation domain portion of the sector risk assessment is to address, at the national level, nine airport perimeter and access control security scenarios. It also stated that the assessment is to integrate all three elements of risk—threat, vulnerability and consequence—and will rely on existing assessment activities, including JVAs. In developing this assessment, it will be important that TSA evaluate whether its current approach to conducting JVAs, which it identifies as one element of its risk assessment efforts, appropriately assesses vulnerabilities across the commercial airport system, and whether additional steps are needed. Since TSA has repeatedly stated the need to develop baseline data on airport security vulnerabilities to enable it to conduct systematic analysis of vulnerabilities on a nationwide basis, TSA could also benefit from exploring the feasibility of leveraging existing assessment information from industry stakeholders to inform this assessment.

DHS also agreed with our second recommendation that a well-developed and well-documented evaluation plan should be part of TSA’s efforts to evaluate and implement future airport security pilot programs. In addition, DHS concurred with our third recommendation that TSA develop milestones for meeting statutory requirements for establishing system requirements and performance standards for the use of biometric airport access control systems. DHS noted that while mandatory use of such systems is not required by statute, TSA is still considering whether it will mandate the use of biometric access control systems at airports, and in the meantime it will continue to encourage airport operators to voluntarily utilize biometrics in their access control systems. We agree that mandatory use of biometric access control systems is not required by statute, but establishing milestones would help guide TSA's continued work with the airport industry to develop and refine existing biometric access control standards. In regard to our fourth recommendation that TSA develop milestones for establishing agency procedures for reviewing airport security requirements imposed through security directives, DHS concurred that milestones are necessary.

Finally, in regard to our fifth recommendation that TSA develop a national strategy for airport security that incorporates key characteristics of effective security strategies, DHS concurred and stated that TSA will develop a national strategy by updating the TS-SSP. DHS stated that TSA intends to solicit input on the plan from its Sector Coordinating Council, which represents key private sector stakeholders from the transportation sector, before releasing the updated TS-SSP in the summer of 2010. However, given that the TS-SSP is to focus on detailing how the NIPP framework will apply to the entire transportation sector, it may not be the most appropriate vehicle for developing a national strategy that addresses the various management issues specific to airport security that we identified in our report. A more effective approach might be to issue the strategy as a stand-alone plan, in keeping with the format TSA has used for its air cargo, passenger checkpoint screening, and SPOT strategies. A stand-alone strategy might better facilitate key stakeholder involvement, focus attention on airport security needs, and allow TSA to more thoroughly address relevant challenges and goals. But irrespective of the format, it will be important that TSA fully address the key characteristics of an effective strategy, as identified in our report. The intent of a national strategy is to provide a unifying framework that guides and integrates stakeholder activities toward desired results, which may be best achieved when planned efforts are clear and sustainable, and transparent enough to ensure accountability. Thus, it is important that the strategy fully incorporate the following characteristics: (1) measurable goals, priorities, and performance measures; (2) program cost information, including the sources and types of resources needed; and (3) plans for coordinating activities among stakeholders, integrating airport security goals and activities with those of other aviation security priorities, and implementing security activities within the agency.

TSA also provided us with technical comments, which we considered and incorporated in the report where appropriate.

We are sending copies of this report to the Secretary of Homeland Security, the Secretary of Transportation, the Assistant Secretary of the Transportation Security Administration, appropriate congressional committees, and other interested parties. The report also is available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any further questions about this report or wish to discuss these matters further, please contact me at (202) 512-4379 or lords@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix IX.

Stephen Lord

Stephen M. Lord
Director, Homeland Security and Justice Issues

List of Requesters

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable John D. Rockefeller, IV
Chairman
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Loretta Sanchez
Chairwoman
Subcommittee on Border, Maritime and Global Counterterrorism
Committee on Homeland Security
House of Representatives

The Honorable Jane Harman
Chairwoman
Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment
Committee on Homeland Security
House of Representatives

The Honorable Sheila Jackson-Lee
Chairwoman
Subcommittee on Transportation Security and Infrastructure Protection
Committee on Homeland Security
House of Representatives

The Honorable Donna M. Christensen
The Honorable Peter A. DeFazio
The Honorable Norman D. Dicks
The Honorable Bob Etheridge
The Honorable James R. Langevin
The Honorable Zoe Lofgren
The Honorable Nita Lowey
The Honorable Ed Markey
The Honorable Kendrick B. Meek
The Honorable Eleanor Holmes Norton
The Honorable Bill Pascrell, Jr.
House of Representatives

Appendix I: Objectives, Scope, and Methodology

This report evaluates to what extent the Transportation Security Administration (TSA) has

- assessed the risk to airport security consistent with the National Infrastructure Protection Plan's (NIPP) risk management framework;
- implemented protective programs to strengthen airport security, and evaluated its worker screening pilot program; and
- established a national strategy to guide airport security decision making.

To evaluate the extent to which TSA has assessed risks for airport perimeter and access control security efforts, we relied on TSA to identify risk assessment activities for these areas, and we then examined documentation for these activities, such as TSA's 2008 Civil Aviation Threat Assessment, and interviewed TSA officials responsible for conducting assessment efforts. We examined the extent to which TSA generally conducted activities intended to assess threats, vulnerabilities, and consequences to the nation's approximately 450 airports. We also reviewed the extent to which TSA's use of these three types of assessments met the NIPP criteria for completing a comprehensive risk assessment. However, while we assessed the extent to which the individual threat and vulnerability assessment activities that TSA identified addressed the area of airport perimeter and access controls, the scope of our work did not include individual evaluations of these activities to determine whether they were consistent with the NIPP criteria for conducting threat and vulnerability assessments. In addition, we reviewed and summarized critical infrastructure and aviation security requirements set out by Homeland Security Presidential Directives 7 and 16, the Aviation and Transportation Security Act (ATSA),[1] and other statutes and related materials. We also examined the individual threat and vulnerability assessment activities and discussed them with senior TSA and program officials, to evaluate how TSA uses this information to set goals and inform its decision making. We compared this information with the NIPP, TSA's Transportation Security Sector-Specific Plan, and our past guidance and reports on recommended risk management practices.[2] In addition, we obtained and analyzed data from TSA regarding joint vulnerability assessments, which are conducted with the Federal Bureau of

[1] Pub. L. No. 107-71, 115 Stat. 597 (2001).

[2] GAO-06-91, GAO-08-904T, and GAO-09-492.

Investigation (FBI), to determine the extent to which TSA has used this information to assess risk to airport perimeter and access control security. We also obtained information on the processes used to schedule and track these activities to determine the reliability with which these data were collected and managed, and we determined that the data were sufficiently reliable for the purposes of this report. We interviewed TSA and FBI officials responsible for conducting joint vulnerability assessments to discuss the number conducted by TSA since 2004, the scope of these assessments, and how they are conducted.

In addition, we interviewed selected TSA officials responsible for risk management and security programs related to airport perimeter and access control to clarify the extent to which TSA has assessed risk in these areas. We selected these officials based upon their relevant expertise with TSA's risk management efforts and its airport perimeter and access control efforts. We also analyzed TSA data on security breaches by calculating the total number of security breaches from fiscal years 2004 through 2008. To determine that the data were sufficiently reliable to present contextual information regarding all breaches to secured areas (including airport perimeters) in this report, we obtained information on the processes used to collect, tabulate, and assess these data, and discussed data quality control procedures with appropriate officials and found that the data were sufficiently reliable for this purpose. Because the data include security breaches that occurred within any type of secured areas, including passenger-related breaches, they are not specific to perimeter and access control security. In addition, the data have not been adjusted to reflect potential issues that could also influence or skew the number of overall breaches, such as annual increases in the number of passengers or specific incidences occurring within individual airports that account for more breaches than others. Furthermore, because TSA does not require its inspectors to enter a description of the breach when documenting an incident, and general reports on breach data do not show much variation between incidences unless a report includes a description of the breach, we did not ask TSA for descriptive information on breaches that occurred.

To evaluate the extent to which TSA has implemented protective programs to strengthen airport security consistent with the NIPP risk management framework, we asked TSA to identify agency-led activities and programs for strengthening airport security. For the purposes of this report, we categorized TSA's responses into four main areas of effort: (1) worker screening pilot program, (2) worker security programs, (3) technology, and (4) general airport security. To determine the extent to which TSA evaluated its worker screening pilot program, we analyzed TSA's final report on it worker screening pilot program, including conclusions and limitations cited by the contractor—the Homeland Security Institute (HSI)—TSA hired to assist with the pilot's design, implementation, and evaluation.[3] We also reviewed standards for internal control in the federal government and our previous work on pilot program development and evaluation to identify accepted practices for ensuring reliable results, including key features of a sound evaluation plan.[4] Further, we analyzed TSA and HSI's documentation of the worker screening pilot program methodology to determine whether TSA and HSI had documented their plans for conducting the program, whether each pilot was carried out in a consistent manner, and if participating airports were provided with written requirements or guidance for conducting the pilots. To evaluate TSA's efforts for its worker security programs, we assessed and summarized relevant program information, operations directives, and standard operating procedures for the Aviation Direct Access Screening Program (ADASP) and enhanced background checks. We also informed this assessment with recent work by the Department of Homeland Security's (DHS) Office of the Inspector General (OIG) regarding worker screening.[5] We reviewed the DHS OIG's methodology and analysis to determine whether its findings were reliable for use in our report. We analyzed TSA's documentation of its background checks to determine if TSA sufficiently addressed relevant ATSA requirements and recommendations from our 2004 report on airport security.[6] We also interviewed TSA officials responsible for worker background checks to determine the agency's efforts to develop a plan to meet outstanding ATSA requirements.

With respect to perimeter and access control technology, we reviewed and summarized TSA documentation and evaluations of the Airport Access Control Pilot Program (AACPP), documentation related to the Airport Perimeter Security (APS) pilot program, and the dissemination of

[3] Transportation Security Administration, *Airport Employee Screening Pilot Program Study: Fiscal Year 2008 Report to Congress*.

[4] GAO/AIMD-00-21.3.1 and GAO-09-45.

[5] Department of Homeland Security, Office of the Inspector General, *TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening*.

[6] GAO-04-728.

information regarding technology to airports. We interviewed officials with the DHS Directorate for Science and Technology, the National Safe Skies Alliance, and RTCA, Inc., regarding research, development, and testing efforts, and challenges and potential limitations of applicable technologies to airport perimeter and access control security. We selected these entities because of their role in the development of such technology. We also interviewed TSA Headquarters officials to obtain views on the nature and scope of technology-related efforts and other relevant considerations, such as how they addressed relevant ATSA requirements and recommendations from our 2004 report, or how they plan to do so. With regard to TSA's efforts for general airport security, we examined TSA's procedures for developing and issuing airport perimeter and access control requirements through security directives and other methods, and analyzed the extent to which TSA disseminated security requirements to airports through security directives. At our request, TSA identified 25 security directives and emergency amendments that imposed requirements related to airport perimeter and access control security, which we examined to identify specific areas of regulation. In addition, we assessed and summarized relevant program information and documentation, such as operations directives, for other programs identified by TSA, such as the Visible Intermodal Prevention and Response (VIPR) program, Screening of Passengers by Observation Techniques (SPOT) program, and the Law Enforcement Officer Reimbursement Program.

To evaluate the extent to which TSA established a national strategy to guide airport security decision making, we considered guidance on effective characteristics for security strategies and planning that we previously reported, Government Performance and Results Act (GPRA) requirements,[7] and generally accepted strategic planning practices for government agencies. In order to evaluate TSA's approach to airport security, we reviewed TSA documents to identify major security goals and subordinate objectives for airport perimeter and access control security, and relevant priorities, goals, objectives, and performance measures. We also analyzed relevant program documentation, including budget, cost, and performance information, including relevant information TSA developed and maintains for the Office of Management and Budget's Performance Assessment Rating Tool. We compared TSA's approach with criteria identified in NIPP, other DHS guidance, GPRA, and other leading

[7] Pub. L. No. 103-62, 107 Stat. 285 (1993).

practices in strategies and planning. We also interviewed relevant TSA program and budget officials, Federal Aviation Administration (FAA) officials, and selected aviation industry officials regarding the cost of airport perimeter and access control security for fiscal years 2004 through 2008.

To determine the extent to which TSA collaborated with stakeholders on airport security activities, and to obtain their insights on airport security operations, costs, and regulation, we interviewed industry officials from the Airports Council International-North America—whose commercial airport members represent 95 percent of domestic airline passenger and air cargo traffic in North America—and from the American Association of Airport Executives—whose members represent 850 domestic airports.[8] We selected these industry associations based on input from TSA and from industry stakeholders, who identified the two associations representing commercial airport operators. We also attended aviation association conferences at which industry officials presented information on national aviation security policy and operations, and we conducted a group discussion with 17 officials representing various airport and aircraft operators and aviation associations to obtain their views regarding key issues affecting airport security. While the views expressed by these industry, airport, and aircraft operator officials cannot be generalized to all airport industry associations and operators, these interviews provided us with additional perspectives on airport security and an understanding of the extent to which TSA has worked and collaborated with airport stakeholders.

We also conducted site visits at nine U.S. commercial airports—Orange County John Wayne Airport, Washington-Dulles International Airport, Miami International Airport, Orlando International Airport, John F. Kennedy International Airport, Westchester County Airport, Logan International Airport, Barnstable Municipal Airport, and Salisbury/Wicomico County Regional Airport. During these visits we observed airport security operations and discussed issues related to

[8] According to the Airports Council International-North America, it represents over 400 aviation-related businesses and approximately 190 governing bodies of more than 400 commercial and general aviation airports in the United States and Canada; collectively, its members enplane about 95 percent of the domestic and nearly 100 percent of international airline passenger and cargo traffic in North America. According to the American Association of Airport Executives, it is the world's largest professional organization for airport executives, with members representing approximately 850 commercial and general aviation airports and the companies and organizations that support airports.

perimeter and access control security with airport officials and on-site TSA officials, including federal security directors (FSD). We selected these airports based on several factors, including airport category, size, and geographical dispersion; whether they faced problems with perimeter and access control security; and the types of technological initiatives tested or implemented. Because we selected a nonprobability sample of airports to visit, those results cannot be generalized to other U.S. commercial airports; however, the information gathered provides insight into TSA and airport programs and procedures. In addition, at Miami International Airport and John F. Kennedy International Airport we conducted separate interviews with airport officials to discuss their ongoing, or anticipated, efforts to implement additional worker screening methods at their respective airports. We also conducted telephone interviews with airport officials and FSDs from four airports that had implemented, or planned to implement, various forms of 100 percent screening of airport workers to discuss their efforts. These were Cincinnati/Northern Kentucky International Airport, Dallas/Fort Worth International Airport, Denver International Airport, and Phoenix Sky Harbor International Airport. While the views of the officials we spoke with regarding additional worker screening methods cannot be generalized to all airport security officials, they provided insight into how airport security programs were chosen and developed. We also conducted an additional site visit at Logan International Airport to observe TSA's implementation of various worker screening methods as part of the agency's worker screening pilot program. While the experiences of this pilot location cannot be generalized to all airports participating in the pilot, we chose this airport based on airport category and the variety of worker screening methods piloted at this location.

We conducted this performance audit from May 2007 through September 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: TSA Actions to Address Selected Statutory Requirements for Airport Security

TSA has taken steps since 2004 to address some of the requirements related to airport perimeter and access control security prescribed by ATSA.[1] The related ATSA requirements, and TSA's actions as of May 2009 to address these requirements, are summarized in table 3.

Table 3: TSA Actions since 2004 to Address Relevant ATSA Requirements through May 2009

ATSA requirements related to airport perimeter and access control security	TSA actions taken in response
Requirement for evaluating airport access controls	
TSA shall, on an ongoing basis, accept and test for compliance with access control requirements, report annually on the findings of the assessments, and assess the effectiveness of penalties in ensuring compliance with security procedures and take any other appropriate enforcement actions when noncompliance is found. See 49 U.S.C. § 44903(g)(2)(D).	The agency has established schedules and developed an analytical approach for completing compliance inspections. In doing so, TSA developed inspection prompts that target critical areas of the airport. TSA officials told us that the agency has not developed measures to assess the effectiveness of its penalties, but believes that its current approach of requiring documentation of issues and prompt corrective action by the operator upon the discovery of noncompliance results in acceptable performance.
Requirements for strengthening the security of airport perimeters and access controls	
Within 6 months after enactment of ATSA (enacted Nov. 19, 2001), TSA shall recommend to airport operators commercially available measures or procedures to prevent access to secure airport areas by unauthorized persons. As part of the assessment, TSA shall review the effectiveness of biometrics systems currently in use, increased surveillance at access points, card- or key-based access systems, and emergency exit systems, as well as specifically targeting the elimination of "piggybacking," where one person follows another through an access point. The assessment shall include a 12-month deployment strategy for currently available technology at all Category X—generally the largest and busiest—airports. Not later than 18 months after enactment, the Secretary of Transportation was to conduct a review of reductions in unauthorized access at Category X airports. See 49 U.S.C. § 44903(j)(1).[a]	TSA officials said that in an effort to assist aviation stakeholders in determining the effectiveness of access control technologies, TSA has provided information to airports on available technology through (1) AACPP, a pilot program designed to test new and emerging access controls technology, and (2) a list of biometric products that meet standards set by TSA. However, TSA officials also stated that while the agency has not yet recommended commercially available measures or a deployment strategy, it plans to implement a second phase of AACPP, which may result in recommended technologies.
TSA shall establish pilot programs in no fewer than 20 airports to test and evaluate technology for providing access control and security protections for closed or secure areas. See 49 U.S.C. § 44903(c)(3).	In 2003 TSA established AACPP, as described above. In December 2006, TSA issued a final report that summarized the results of the 20 pilot projects involved in the program.

[1] Pub. L. No. 107-71, 115 Stat. 597 (2001).

ATSA requirements related to airport perimeter and access control security	TSA actions taken in response
TSA shall develop a plan to provide technical support and financial assistance to airports with less than 1 percent of the total annual enplanements for the most recent calendar year for which data are available, to enhance security operations and to defray the costs of such enhancements. See Pub. L. No. 107-71, § 106(b)(1), 115 Stat. 571, 609.	According to TSA officials, the agency has in part met this requirement by providing technical assistance through AACPP, the APS pilot program, and the Law Enforcement Officer Reimbursement Program. However, officials explained that as of May 2009 the agency had not yet developed a plan to provide technical information and funding to small- and medium-sized airports, because TSA has not been specifically directed to obligate funding for this purpose, and that its resources and management attention have focused on requirements for which it has direct responsibility and deadlines, including passenger and baggage screening.
Requirements for reducing the risks posed by airport workers	
TSA shall, as part of the employment investigation for escorted or unescorted access to aircraft or secured areas of an airport, include a review of available law enforcement databases and records of other government and international agencies, to the extent determined practicable. See 49 U.S.C. § 44936.	While TSA requires background checks—which include fingerprint and name-based checks—on all workers with unescorted access to secured airport areas, it does not require such checks for workers who have regularly escorted access. According to TSA officials, it is not necessary to conduct checks on workers who have regularly escorted access because the agency has taken other steps that adequately address the threat that may be posed by regularly escorted workers, such as random screening. In addition, in October 2007, TSA issued a security directive that contained a requirement limiting the number of workers who can escort nonauthorized workers. TSA officials also stated that airports typically seal off or isolate the area where workers with escorted access are located.
TSA shall require scheduled passenger carriers, and airports operating under TSA-approved security programs, to develop security awareness training programs for airport employees; ground crews; gate, ticket, and curbside agents of the air carriers; and other individuals employed at such airports. See Pub. L. No. 107-71, § 106(e), 115 Stat. 571, at 610.	According to TSA officials, this requirement is addressed through a security directive that requires airports to implement a security awareness plan to keep employees, contractors, and new hires informed of the increased threat to airport security and their individual security responsibilities. Workers must report suspicious items or activities that come to their attention at the airport to the appropriate official, in accordance with local procedures. In addition, according to TSA officials, TSA-approved aircraft operator programs should contain specific and detailed requirements for initial and recurrent security training of aircraft workers.
TSA shall require vendors having direct access to the airfield and aircraft to develop their own security programs. See 49 U.S.C. § 44903(h)(4)(D).	According to TSA officials, this requirement is addressed through the airport security program plans that airport operators are required by law and regulation to develop; these plans are to include vendor operations. Further, TSA officials noted that airport security directives require vendor workers who have access to a secured area to undergo fingerprint-based criminal history background checks. In addition, according to officials, airports are required to inspect all vendor deliveries, vendor employees, and delivery personnel. TSA officials noted that the agency can assist airports in these efforts by screening employees though ADASP.

ATSA requirements related to airport perimeter and access control security	TSA actions taken in response
TSA shall require, as soon as practicable after enactment, screening or inspection of all persons, vehicles, equipment, goods, and property before they enter secured areas of airports operating under TSA-approved security programs. See 49 U.S.C. § 44903(h)(4)(A).	TSA officials stated that the agency has met this requirement through collective airport security activities, such as airport worker background checks and the random screening of airport workers and vehicles.

Sources: Pub. L. No. 107-71, §§ 106, 136, 138, 115 Stat. 597, 608-10, 36-37, 39-41 (2001), and GAO summary and analysis of TSA actions taken.

[a] Pursuant to the Homeland Security Act of 2002, TSA transferred from the Department of Transportation to the newly established DHS. See Pub. L. No. 107-296, § 403, 116 Stat. 2135, 2178 (2002).

Appendix III: TSA Also Uses Compliance Inspections and Covert Testing to Detect Possible Airport Security Vulnerabilities

TSA officials told us that they use the results of compliance inspections and covert testing to augment their assessment of potential vulnerabilities in airport security. Compliance inspections examine a regulated entity's—such as an airport operator or air carrier—adherence to federal regulations, which TSA officials say they use to determine if airports adequately address known threats and vulnerabilities.[1] According to TSA, while regulatory compliance is just one dimension of airport security, compliance with federal requirements allows TSA to determine the general level of security within an airport. As a result, according to TSA, compliance with regulations suggests less vulnerability within an airport and, conversely, failure to meet critical compliance rates suggests the likelihood of a larger problem within an airport and helps the agency identify and assess vulnerabilities. TSA allows its inspectors to conduct compliance inspections based on observations of various activities, such as ADASP, VIPR, and local covert testing, and to conduct additional inspections based on vulnerabilities identified through assessments or the results of regular inspections.

Covert tests are any test of security systems, personnel, equipment, and procedures to obtain a snapshot of the effectiveness of that security measure, and they are used to improve airport performance, safety, and security. TSA officials stated that covert testing assists the agency in identifying airport vulnerabilities because such tests are designed based on threat assessments and intelligence to approximate techniques that terrorists may use to exploit gaps in airport security. TSA conducts four types of covert tests for airport access controls:

- **Access to security identification display areas (SIDA):** TSA inspectors not wearing appropriate identification attempt to penetrate SIDA access points, such as boarding gates, employee doors, and other entrances.
- **Access to air operations areas (AOA):** TSA inspectors not wearing appropriate identification attempt to penetrate AOA via access points from public areas, such as perimeter gates and cargo areas.

[1] For example, pursuant to ATSA, TSA shall, on an ongoing basis, accept and test for compliance with access control requirements, report annually on the findings of the assessments, assess the effectiveness of penalties in ensuring compliance with security procedures, and take any other appropriate enforcement actions when noncompliance is found. See 49 U.S.C. § 44903(g)(2)(D).

- **Access to aircraft:** TSA inspectors not wearing appropriate identification (or not carrying valid boarding passes) attempt to penetrate passenger access points that lead to aircraft from sterile areas, such as boarding gates, employee doors, and jet ways.

- **SIDA challenges:** Once inside a SIDA, TSA inspectors attempt to walk around these areas, such as the tarmac and baggage loading areas, without displaying appropriate identification.

TSA also requires FSDs to conduct similar, locally controlled tests of access controls to ensure compliance and identify possible vulnerabilities with airport security. These tests are selected by the FSDs and based on locally identified risks and can include challenging procedures in the secure area, piggybacking (following authorized airport workers into secured areas), and attempting to access an aircraft from sterile area.

According to TSA officials, the agency uses the results of its covert tests to inform decision making for airport security, but officials could not provide examples of how this information has specifically informed past decisions.[2]

[2] See GAO, *Transportation Security: TSA Has Developed a Risk-Based Covert Testing Program, but Could Better Mitigate Aviation Security Vulnerabilities Identified Through Covert Tests*, GAO-08-958 (Washington, D.C.: Aug. 8, 2008). TSA conducts national covert tests of three aspects of aviation security at a commercial airport: (1) passenger checkpoint, (2) checked baggage, and (3) access controls to secure areas and airport perimeters.

Appendix IV: Costs for Airport Security

Various TSA offices and programs contribute to the overall operations and costs of airport perimeter and access control security. According to TSA officials, the agency does not develop a cost estimate specific to perimeter and access control security because such efforts are often part of broader security activities or related programs—for example, VIPR and SPOT are also used for passenger screening. As a result, it is difficult to identify what percentage of program costs has been expended on airport perimeter and access control security activities. At our request, TSA officials identified the estimated spending related to perimeter and access control security programs from fiscal years 2004 through 2008 (see table 4).[1]

Table 4: Summary of TSA-Identified Costs Related to Airport Security, Fiscal Years 2004–2008

Present year dollars in millions

Program/office	**FY04**	**FY05**	**FY06**	**FY07**	**FY08**	**Total**
Office of Law Enforcement/ Federal Air Marshal Service						
Joint Vulnerability Assessment Program	$0.03	$0.08	$0.06	$0.10	$0.08	**$0.35**
Law Enforcement Reimbursement Program	64.24	63.61	67.36	66.22	66.90	**$328.33**
Office of Security Operations						
ADASP[a]	N/A	N/A	N/A	$38.00	$70.60	**$108.60**
SPOT[b]	N/A	N/A	$5.01	$21.46	$87.07	**$113.54**
VIPR	N/A	N/A	N/A	$1.94	NSI[c]	**NSI**
Compliance Inspections	N/A	68.34	70.65	74.30	75.70	**$288.99**
Office of Transportation Threat Assessment and Credentialing	N/A	N/A	2.00	2.00	2.00	**$6.00**
Office of Intelligence Special Operations Covert Test Program	0.18	0.15	0.06	0.12	0.05	**$0.56**
Office of Transportation Sector Network Management[d]	N/A	N/A	NSI	NSI	NSI	**NSI**
Total Identified Costs						**$846.37**

Source: GAO summary of TSA data.

Legend: N/A = not applicable; NSI = not separately identified.

[1] In addition to the costs in table 4, TSA officials identified a total of $49.2 million in estimated costs from fiscal years 2003 through 2008 related to pilot programs specific to airport security: $19.6 million to AACPP for fiscal years 2003 through 2005, $16.9 million for the Airport Terminal Security Grant Program for fiscal years 2004 and 2005, $5.0 million for the APS pilot program in fiscal year 2006, and $7.7 million for the worker screening pilot program in fiscal year 2008.

Notes: This table includes funds either obligated or expended by TSA for programs and activities related to airport perimeter and access control security (figures rounded to the nearest one hundredth). However, many of these programs and activities also include efforts that apply to other areas of aviation security. For example, compliance inspections are used to assess the extent to which airports comply with perimeter and access control requirements, as well as to assess the extent to which air carriers comply with other TSA regulations. Because of rounding, numbers may not add to totals.

[a] The ADASP fiscal year 2007 figure is an estimate based upon ADASP staff days allocated to all commercial airports calculated by using the average cost of 1 staff day devoted to ADASP activities.

[b] Cost figures for SPOT are TSA's estimates of expenditures for the respective fiscal years; they do not reflect allocations. TSA allotted $40.8 million to SPOT activities for fiscal year 2007 and $144.1 million for fiscal year 2008. According to TSA officials, approximately $80 million that the agency initially allotted for SPOT activities in fiscal years 2007 and 2008 was not spent on the program, but was expended for general transportation security officer performance, compensation, and benefits.

[c] NSI indicates that the specific costs for these programs were unknown because the activities were elements of a larger program and could not be separately identified by TSA. For example, in fiscal year 2008 TSA was allocated $20 million for VIPR, but the amount to be applied to airport perimeter and access controls security was not separately identified.

[d] TSA officials said that they did not track and could not separately identify the estimated costs for perimeter and access control–related activities conducted by the Office of Transportation Sector Network Management in fiscal years 2006 through 2008 because such activities are part of normal staff hour and contractor support costs. According to TSA officials, such activities include those related to SIDA II, the APS pilot program, and security directive development and implementation.

Airports can receive funding for purposes related to perimeter and access control security via grants awarded through FAA's Airport Improvement Program. TSA officials also told us that the agency generally does not collect or track cost information for airport security efforts funded through the Airport Improvement Program.[2] This program is one of the principal sources of funding for airport capital improvements in the United States, providing approximately $3 billion in grants annually to enhance airport capacity, safety, and environmental protection, as well as perimeter security. According to FAA officials, many factors are considered when awarding grants to airports for perimeter security enhancements, although security projects required by statute or regulation receive the highest priority. Projects that receive funding have included computerized access controls for ramps, infrastructure improvements to house central computers, surveillance systems, and perimeter fencing. According to FAA, more than $365 million in airport perimeter and access

[2] TSA assumed primary responsibility for aviation security from FAA in February 2002; FAA-administered Airport Improvement Program grants are available to airports for limited security purposes. According to TSA officials, TSA monitors $5 million of this funding awarded annually to the National Safe Skies Alliance (a nonprofit membership consortium that tests airport security equipment, systems, and processes at airports throughout the United States and abroad). FAA provides not less than $5 million each fiscal year for this grant. According to FAA and TSA officials, the National Safe Skies Alliance uses these funds to test innovative security systems and technology.

control–related grants were provided through the Airport Improvement Program for fiscal years 2004 through 2008.

TSA officials also told us that the agency does not track funds spent by individual airport operators to enhance or maintain perimeter and access control security. In 2009 the Airports Council International-North America—an aviation industry association—surveyed commercial airports regarding the funding needed for airport capital projects from 2009 to 2013. As part of this effort, the association surveyed airport operators on the amount of funds they planned to expend on airport security as a percentage of their overall budgets.[3] The association reported that planned airport operator spending on airport security, as a percentage of total spending, ranged from 3.8 percent (about $2 billion) for large hub airports to 3.9 percent (about $230 million) for small hub airports.[4] The association surveys did not include information on the types of security projects undertaken by airports. However, during our site visits we obtained data from selected airport operators on the costs of perimeter and access control security projects they had recently concluded or estimated costs for projects in progress. Examples of airport spending on perimeter and access control security include

- $30 million to install a full biometric access system;
- $6.5 million to install an over 8,000-foot-long blast/crash resistant wall along the airport perimeter;
- $8 million to install over 680 bollards in front of passenger terminals and vehicle access points; and
- $3 million to develop and install an infrared intrusion detection system.

[3] Airports Council International-North America, *Airport Capital Development Cost Survey 2009-2013* (Washington, D.C., February 2009).

[4] In 2007, for the period 2007 through 2011, the association reported that airport operator spending ranged from 6.6 percent (about $3 billion) for large hub airports to 4.8 percent (about $300 million) for small hub airports. The Airports Council International-North America used its own survey data and FAA National Plan Integrated Airport System data to develop these estimates. Past GAO work explains the differences between the association's survey estimates and FAA's data. See GAO, *Airport Finance: Preliminary Analysis of Proposed Changes in the Airport Improvement Program May Not Resolve Funding Needs for Smaller Airports*, GAO-07-617T (Washington, D.C.: Mar. 28, 2007).

Appendix V: TSA Worker Screening Pilot Program

From May through July 2008 TSA implemented worker screening pilots at seven airports in accordance with the Explanatory Statement accompanying the DHS Appropriations Act, 2008 (see table 5 for a summary of text directing the worker screening pilot program). At three airports, TSA conducted 100 percent worker screening—inspections of all airport workers and vehicles entering secure areas; at four others TSA randomly screened 20 percent of workers and tested other enhanced security measures. Screening of airport workers was to be done at either the airport perimeter or the passenger screening checkpoints. TSA was directed to collect data on the methods it utilized, and evaluate the benefits, costs, and impacts of 100 percent worker screening to determine the most effective and cost-efficient method of addressing and deterring potential security risks posed by airport workers.

Table 5: Summary of Explanatory Text Directing the Worker Screening Pilot Program

Categories	Explanatory text
Funding	$15,000,000.
Duration	TSA shall screen all airport workers at three airports for no less than 90 days.
Implementation	Undertake other screening methods at up to four additional airports.
Alternatives	Other methods to enhance screening could include physical inspections, behavioral recognition, biometric access controls, cameras, and body imaging.
Data collection	TSA shall collect data on the benefits, costs, and impacts of 100 percent airport worker screening as well as on the other methods utilized.
Reporting results	TSA shall report to the Committees on Appropriations of the Senate and House of Representatives on (1) the results of the pilots, including the average wait times at screening checkpoints for passengers and workers; (2) the estimated cost of the infrastructure and personnel necessary to implement a screening program for airport workers at all U.S. commercial service airports in order to meet a 10-minute standard for processing passengers and workers through screening checkpoints; (3) the ways in which the current methods for screening airport workers could be strengthened; and (4) the impact of screening airport workers on other security-related duties at airports. TSA shall provide an interim briefing to the committees on the progress and results of these pilots not later than September 1, 2008.

Source: Explanatory Statement accompanying Division E of the Consolidated Appropriations Act, 2008; Pub. L. No. 110-161, 121 Stat. 1844, 2042 (2007), at 1048.

The enhanced measures that TSA tested at the four airports not implementing 100 percent screening are summarized below:

- **Employee training***:* TSA provided a security awareness training video, which all SIDA badgeholders were required to complete. According to TSA, the training intended reduce security breaches by increasing workers' understanding of their security responsibilities and awareness of threats and abnormal behaviors.

- **Behavioral recognition training***:* TSA provided funding to participating airports to teach select law enforcement officers and airport personnel to identify potentially high-risk individuals based on their behavior. A condensed version of the SPOT course, this training was intended to equip personnel with skills to enhance existing duties, according to TSA officials.

- **Targeted physical inspections***:* TSA conducted random inspections of vehicles and individuals entering the secured areas of airports to increase the coverage of ADASP. Inspections consisted of bag, vehicle, and identification checks; scanning bottled liquids; and random security sweeps of specific airport areas.

- **Deployment of technology***:* TSA employed additional technology at selected airports to assist with the screening of employees, such as walk-through and handheld metal detectors, bottled liquid scanners, and explosive detection systems. TSA also tested biometric access control systems at selected airports.

Appendix VI: Additional TSA Efforts to Improve General Airport Security

VIPR

According to TSA, VIPR operations augment existing airport security activities, such as ADASP, and provide a visual deterrent to terrorist or other criminal activity. VIPR was first implemented in 2005, and according to TSA officials, VIPR operations are deployed through a risk-based approach and in response to specific intelligence information or known threats. In a VIPR operation, TSA officials, including transportation security officers and inspectors, behavioral detection officers, bomb appraisal officers, and federal air marshals work with local law enforcement and airport officials to temporarily enhance aviation security. According to TSA officials, VIPR operations for perimeter and access control security can include random inspections of individuals, property, and vehicles, as well as patrols of secured areas and random checks to ensure that employees have the proper credentials. TSA officials told us that although they do not know how many VIPR deployments have specifically addressed airport perimeter and access control security, from March 2008 through April 2009 TSA performed 1,042 commercial and general aviation airport or cargo VIPR operations. According to TSA officials, the majority of these operations involved the observation and patrolling of secured airport areas and airport perimeters. As of May 2009 TSA officials also said that the agency is in the process of enhancing its VIPR database to more accurately capture and track specific operational objectives, such as enhancing the security of airport perimeters and access controls, and developing an estimated time frame for completing this effort.[1]

SPOT

Since 2004 TSA has used SPOT—a passenger screening program in which behavior detection officers observe and analyze passenger behavior to identify potentially high-risk individuals—to determine if an individual or individuals may pose a risk to aircraft or airports. Although SPOT was

[1] TSA uses VIPR to augment security in transportation areas other than aviation. As discussed in our June 2009 report on mass transit and passenger rail security we found that opinions regarding VIPR's additional security value and effectiveness for that mode were varied among municipal transit agency officials (see GAO, *Transportation Security: Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, but Opportunities Exist to Strengthen Federal Strategy and Programs*, GAO-09-678 (Washington, D.C.: June 24, 2009)). For example, some officials told us that they welcomed the additional manpower of VIPR teams, while others reported that deploying VIPR for a single day did not significantly enhance security. While airport operators did not raise such issues to us, lessons learned from TSA's application of VIPR in other modes of transportation can inform its use in airport security. TSA officials agreed that VIPR has experienced challenges and said that they have taken steps to address these issues, such as providing information to help agencies customize VIPR operations to their needs.

originally designed for passenger screening, TSA officials stated that FSDs can also use behavior detection officers to assess worker behavior as they pass through the passenger checkpoint, as part of random worker screening operations or as part of VIPR teams deployed at an airport. However, TSA officials could not determine how often behavior detection officers have participated in random worker screening or VIPR operations, or identify which airports have used behavior detection officers for random worker screening. According to TSA officials, the agency is in the process of redesigning its data collection efforts and anticipates that it will be able to more accurately track this information in the future, though officials did not provide a time frame for doing so. TSA officials also told us that when participating in random worker screening, behavior detection officers observe workers for suspicious behavior as they are being screened and may engage workers in casual conversation to assess potential threats. According to TSA officials, the agency has provided behavior detection training to law enforcement personnel as part of its worker screening pilot program, as well as to selected airport security and operations personnel at more than 20 airports.[2] We currently have ongoing work assessing SPOT, and will issue a report on this program at a later date.

Law Enforcement Officer Reimbursement Program

TSA undertakes efforts to facilitate the deployment of law enforcement personnel authorized to carry firearms at airport security checkpoints, and in April 2002, the Law Enforcement Officer Reimbursement Program was established to provide partial reimbursement for enhanced, on-site law enforcement presence in support of the passenger screening checkpoints. Since 2004, the program has expanded to include law enforcement support along the perimeter and to assist with worker screening. According to TSA, the program is implemented through a cooperative agreement process that emphasizes the ability of both parties to identify and agree as to how law enforcement officers will support the specific security requirements at an airport. For example, the FSD, in consultation with the airport operator and local law enforcement, may determine that rather than implementing fixed-post stationing of law enforcement officers, it

[2] For fiscal year 2008, TSA has allocated approximately $100 million to expand SPOT beyond fiscal year 2007 levels, resulting in a total program cost of approximately $140 million for fiscal year 2008. According to agency officials, as of April 2009 TSA had stationed approximately 2,836 behavior detection officers at all Category X, I, and II airports and one Category III airport; no SPOT teams had been assigned to Category IV airports.

may be more appropriate to implement flexible stationing of law enforcement officers. TSA may also provide training or briefings on an as-needed basis on relevant security topics, including improvised explosive device recognition, federal criminal statutes pertinent to aviation security, and procedures and processes for armed law enforcement officers. Awards made under the reimbursement program are subject to the availability of appropriated funds, among other things, and are to supplement not supplant state and local funding. According to TSA officials, however, no applicant has been denied funds based on lack of appropriated funds.

Appendix VII: Alternative Methods Available to Assist TSA in Assessing the Effectiveness of Its Actions to Strengthen Airport Security

Program evaluation methods exist whereby TSA could attempt to assess whether its activities are meeting intended objectives. These methods center on reducing the risk of both external and internal threats to the security of airport perimeters and access controls, and seek to use information and resources available to help capture pertinent information.

First, recognizing that there are challenges associated with measuring the effectiveness of deterrence-related activities, the NIPP's Risk Management Framework provides mechanisms for qualitative feedback that although not considered a metric, could be applied to augment and improve the effectiveness and efficiency of protective programs and activities. For example, working with stakeholders—such as airport operators and other security partners—to identify and share lessons learned and best practices across airports could assist TSA in better tailoring its efforts and resources and continuously improving security. Identifying a range of qualitative program information—such as information gathered through vulnerability assessment activities or compliance inspections—could also allow TSA to determine whether activities are effective. As discussed in appendix III, compliance inspections and covert tests could be used to identify noncompliance with regulations or security breaches within designated secured areas. For example, TSA could use covert tests to determine if transportation security officers are following TSA procedures when screening airport workers or whether certain worker screening procedures detect prohibited items. However, in order to improve the usefulness of this technique, we previously recommended to TSA that the agency develop a systematic process for gathering and analyzing specific causes of all covert testing failures, record information on processes that may not be working properly during covert tests, and identify effective practices used at airports that perform well on covert tests.[1]

Second, as TSA has already begun to do with some activities, it could use data it already collects to identify trends and establish baseline data for a future comparison of effectiveness.[2] For example, a cross-sectional analysis of the number of workers caught possessing prohibited items at specific worker screening locations over time, while controlling for variables such as increased law enforcement presence or airport size,

[1] GAO-08-958.

[2] Analyzing trends over time allows agencies to establish a baseline for security activities. Examining trends can assist in identifying what specific security measures in place allowed for certain security breaches to occur or increase.

could provide insights into what type of security activities help to reduce the possession of prohibited items. Similarly, an examination of airport workers apprehended, fired, or referred to law enforcement while on the job could provide insights into the quality of worker background checks and security threat assessments. Essentially, the these types of analyses provide a useful context for drawing conclusions about whether certain security practices are reasonable and appropriate given certain conditions and, gradually, with the accumulation of relevant data, should allow TSA to start identifying cause-and-effect relationships.

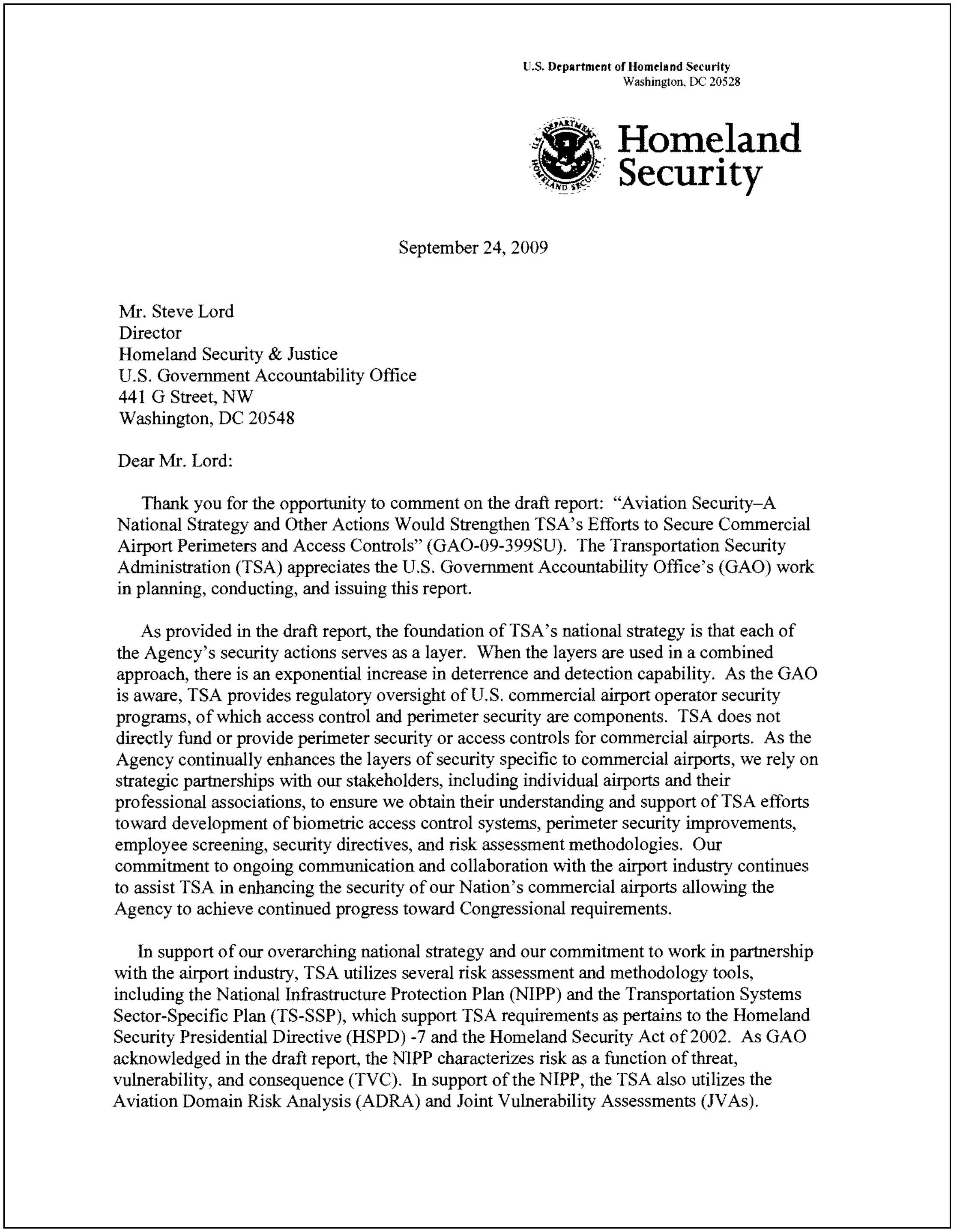
Third, according to the Office of Management and Budget (OMB), the use of proxy measures may also allow TSA to determine how well its activities are functioning.[3] Proxy measures are indirect measures or indicators that approximate or represent the direct measure. TSA could use proxy measures to address deterrence, other security goals as identified above, or a combination of both. According to OMB, proxy measures are to be correlated to an improved security outcome, and the program should be able to demonstrate—for example, through the use of modeling—how the proxies tie to the eventual outcome. The Department of Transportation has also highlighted the need for proxy measures when assessing maritime security efforts pertaining to deterrence.[4] For example, according to the Department of Transportation, while a direct measure of access to seaports might be the number of unauthorized intruders detected, proxy measures for seaport access may include related information on gates and guards—combined with crime statistics relating to unauthorized entry in the area of the port—to support a broader view of port security. In terms of aviation security, because failure to prevent a worker from placing a bomb on a plane could be catastrophic, proxy measures may include information on access controls, worker background checks, and confiscated items. Proxy measures could also include information on aircraft operators' efforts to secure the aircraft. In using a variety of proxy measures, failure in any one of the identified measures could provide an indication on the overall risk to security.

[3] Office of Management and Budget, *Performance Measure Challenges and Strategies* (Washington, D.C., June 18, 2003).

[4] Department of Transportation, *Assessment of Performance Measures for Security of Maritime Transportation Network, Port Security Metrics: Proposed Measurement of Deterrence Capability.*

Lastly, the use of likelihood, or “what-if scenarios,” which are used to describe a series of steps leading to an outcome, could allow TSA to assess whether potential activities and efforts effectively work together to hypothetically achieve a positive outcome. For example, the development of such scenarios could help TSA to consider whether an activity’s procedures could be modified in response to identified or projected changes in terrorist behaviors, or if an activity’s ability to reduce or combat a threat is greater if used in combination with other activities.

Appendix VIII: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

September 24, 2009

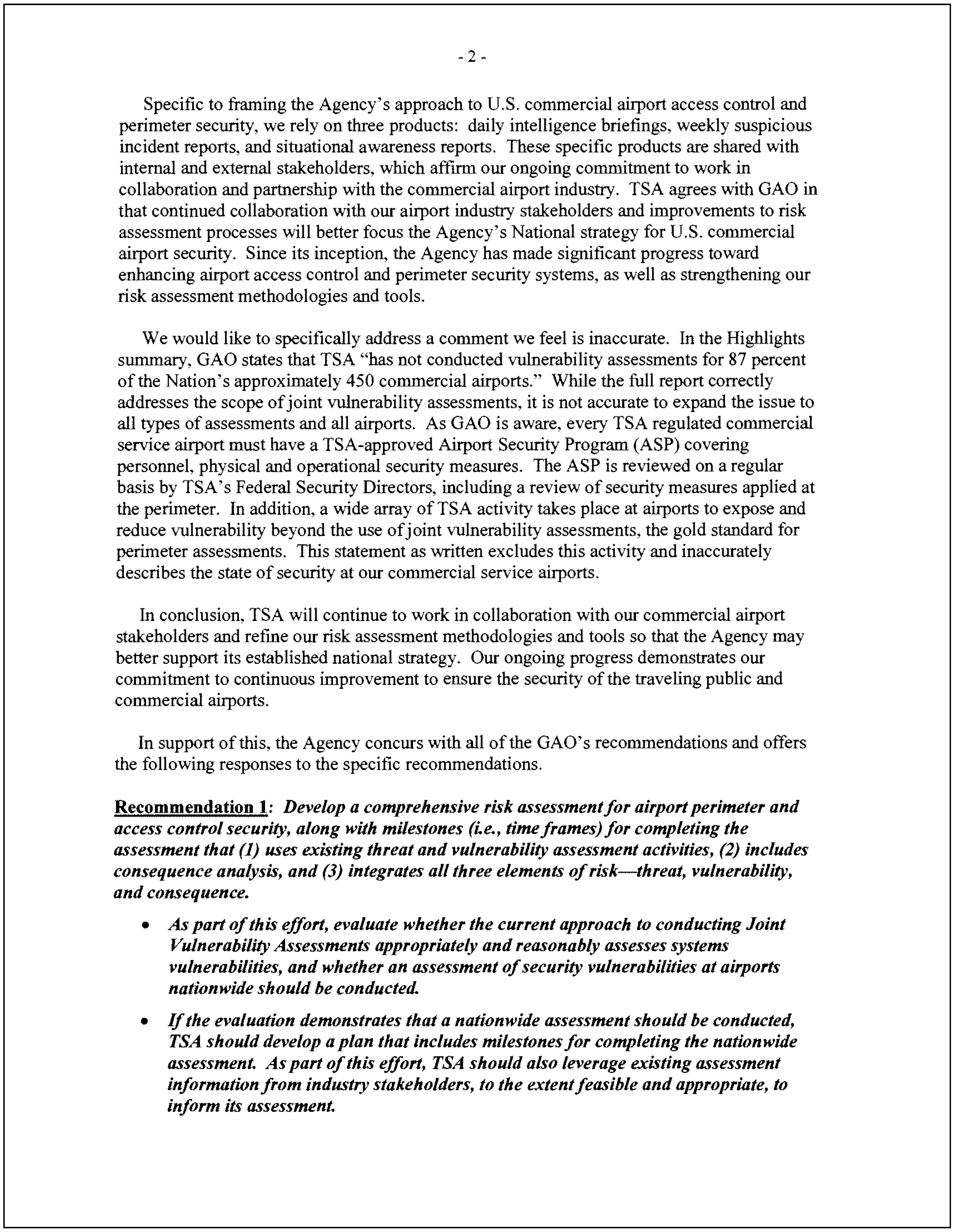
Mr. Steve Lord
Director
Homeland Security & Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Lord:

Thank you for the opportunity to comment on the draft report: "Aviation Security–A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls" (GAO-09-399SU). The Transportation Security Administration (TSA) appreciates the U.S. Government Accountability Office's (GAO) work in planning, conducting, and issuing this report.

As provided in the draft report, the foundation of TSA's national strategy is that each of the Agency's security actions serves as a layer. When the layers are used in a combined approach, there is an exponential increase in deterrence and detection capability. As the GAO is aware, TSA provides regulatory oversight of U.S. commercial airport operator security programs, of which access control and perimeter security are components. TSA does not directly fund or provide perimeter security or access controls for commercial airports. As the Agency continually enhances the layers of security specific to commercial airports, we rely on strategic partnerships with our stakeholders, including individual airports and their professional associations, to ensure we obtain their understanding and support of TSA efforts toward development of biometric access control systems, perimeter security improvements, employee screening, security directives, and risk assessment methodologies. Our commitment to ongoing communication and collaboration with the airport industry continues to assist TSA in enhancing the security of our Nation's commercial airports allowing the Agency to achieve continued progress toward Congressional requirements.

In support of our overarching national strategy and our commitment to work in partnership with the airport industry, TSA utilizes several risk assessment and methodology tools, including the National Infrastructure Protection Plan (NIPP) and the Transportation Systems Sector-Specific Plan (TS-SSP), which support TSA requirements as pertains to the Homeland Security Presidential Directive (HSPD) -7 and the Homeland Security Act of 2002. As GAO acknowledged in the draft report, the NIPP characterizes risk as a function of threat, vulnerability, and consequence (TVC). In support of the NIPP, the TSA also utilizes the Aviation Domain Risk Analysis (ADRA) and Joint Vulnerability Assessments (JVAs).



Specific to framing the Agency's approach to U.S. commercial airport access control and perimeter security, we rely on three products: daily intelligence briefings, weekly suspicious incident reports, and situational awareness reports. These specific products are shared with internal and external stakeholders, which affirm our ongoing commitment to work in collaboration and partnership with the commercial airport industry. TSA agrees with GAO in that continued collaboration with our airport industry stakeholders and improvements to risk assessment processes will better focus the Agency's National strategy for U.S. commercial airport security. Since its inception, the Agency has made significant progress toward enhancing airport access control and perimeter security systems, as well as strengthening our risk assessment methodologies and tools.

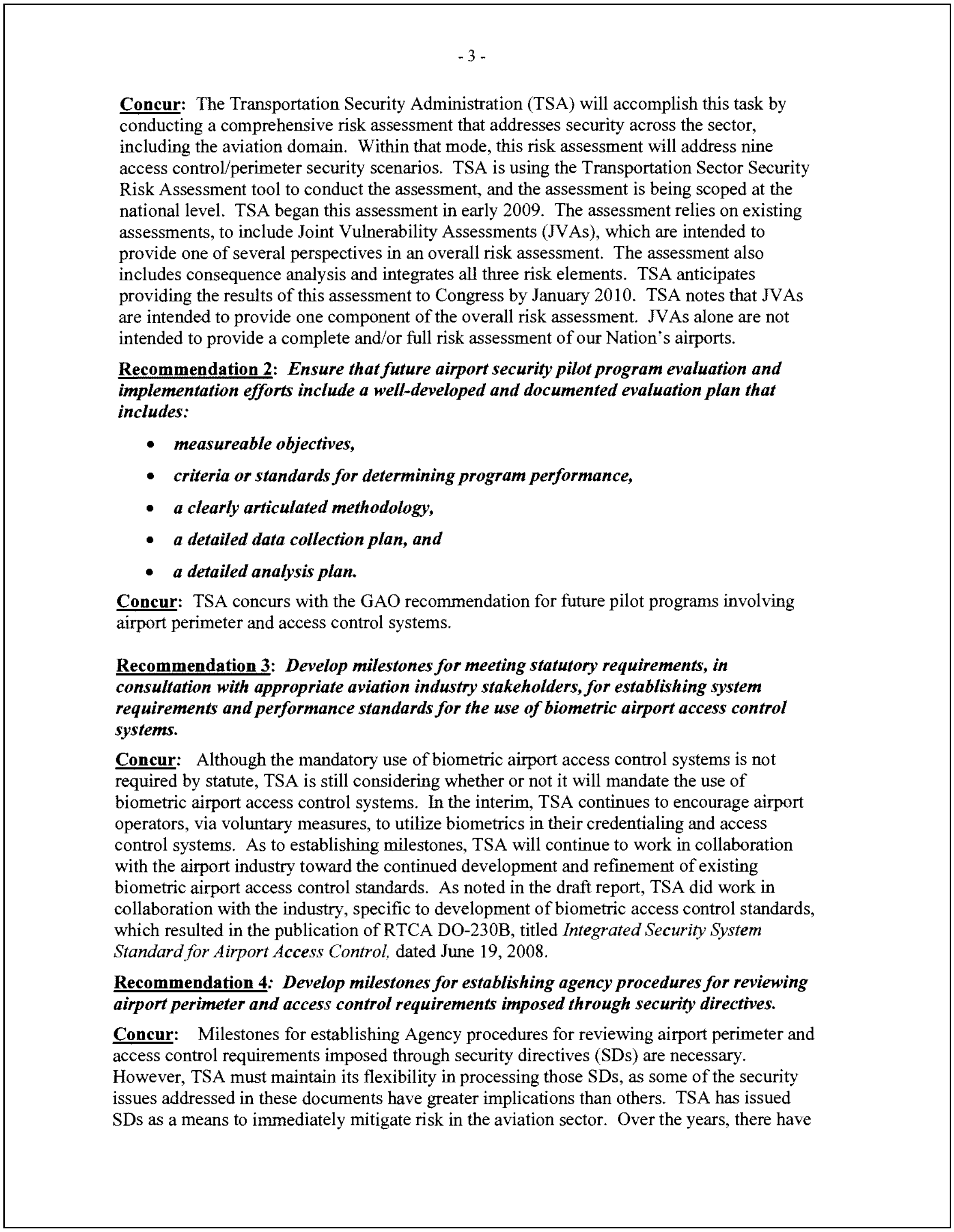
We would like to specifically address a comment we feel is inaccurate. In the Highlights summary, GAO states that TSA "has not conducted vulnerability assessments for 87 percent of the Nation's approximately 450 commercial airports." While the full report correctly addresses the scope of joint vulnerability assessments, it is not accurate to expand the issue to all types of assessments and all airports. As GAO is aware, every TSA regulated commercial service airport must have a TSA-approved Airport Security Program (ASP) covering personnel, physical and operational security measures. The ASP is reviewed on a regular basis by TSA's Federal Security Directors, including a review of security measures applied at the perimeter. In addition, a wide array of TSA activity takes place at airports to expose and reduce vulnerability beyond the use of joint vulnerability assessments, the gold standard for perimeter assessments. This statement as written excludes this activity and inaccurately describes the state of security at our commercial service airports.

In conclusion, TSA will continue to work in collaboration with our commercial airport stakeholders and refine our risk assessment methodologies and tools so that the Agency may better support its established national strategy. Our ongoing progress demonstrates our commitment to continuous improvement to ensure the security of the traveling public and commercial airports.

In support of this, the Agency concurs with all of the GAO's recommendations and offers the following responses to the specific recommendations.

<u>Recommendation 1</u>: ***Develop a comprehensive risk assessment for airport perimeter and access control security, along with milestones (i.e., time frames) for completing the assessment that (1) uses existing threat and vulnerability assessment activities, (2) includes consequence analysis, and (3) integrates all three elements of risk—threat, vulnerability, and consequence.***

- ***As part of this effort, evaluate whether the current approach to conducting Joint Vulnerability Assessments appropriately and reasonably assesses systems vulnerabilities, and whether an assessment of security vulnerabilities at airports nationwide should be conducted.***
- ***If the evaluation demonstrates that a nationwide assessment should be conducted, TSA should develop a plan that includes milestones for completing the nationwide assessment. As part of this effort, TSA should also leverage existing assessment information from industry stakeholders, to the extent feasible and appropriate, to inform its assessment.***



Concur: The Transportation Security Administration (TSA) will accomplish this task by conducting a comprehensive risk assessment that addresses security across the sector, including the aviation domain. Within that mode, this risk assessment will address nine access control/perimeter security scenarios. TSA is using the Transportation Sector Security Risk Assessment tool to conduct the assessment, and the assessment is being scoped at the national level. TSA began this assessment in early 2009. The assessment relies on existing assessments, to include Joint Vulnerability Assessments (JVAs), which are intended to provide one of several perspectives in an overall risk assessment. The assessment also includes consequence analysis and integrates all three risk elements. TSA anticipates providing the results of this assessment to Congress by January 2010. TSA notes that JVAs are intended to provide one component of the overall risk assessment. JVAs alone are not intended to provide a complete and/or full risk assessment of our Nation's airports.

Recommendation 2: ***Ensure that future airport security pilot program evaluation and implementation efforts include a well-developed and documented evaluation plan that includes:***

- ***measureable objectives,***
- ***criteria or standards for determining program performance,***
- ***a clearly articulated methodology,***
- ***a detailed data collection plan, and***
- ***a detailed analysis plan.***

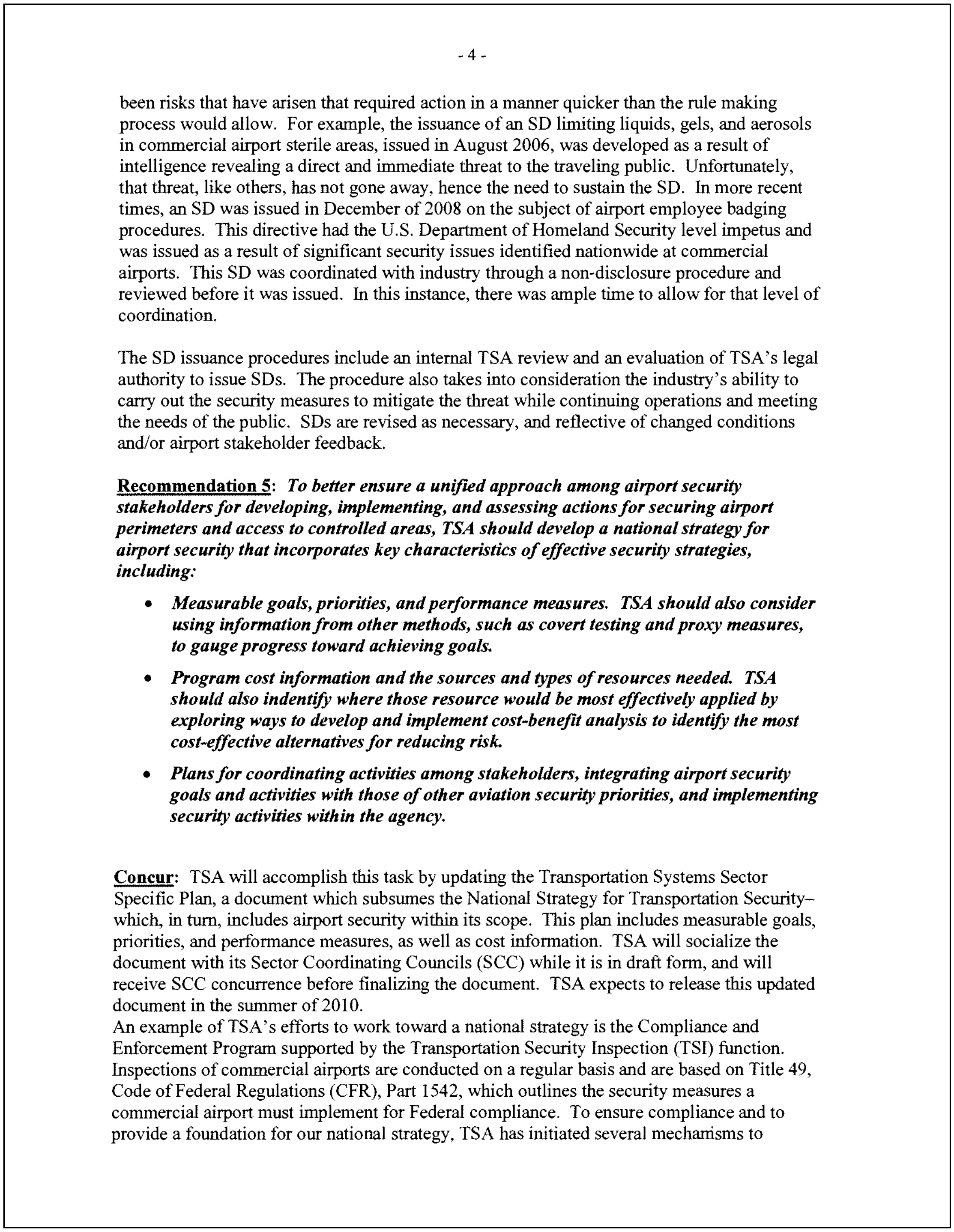
Concur: TSA concurs with the GAO recommendation for future pilot programs involving airport perimeter and access control systems.

Recommendation 3: ***Develop milestones for meeting statutory requirements, in consultation with appropriate aviation industry stakeholders, for establishing system requirements and performance standards for the use of biometric airport access control systems.***

Concur: Although the mandatory use of biometric airport access control systems is not required by statute, TSA is still considering whether or not it will mandate the use of biometric airport access control systems. In the interim, TSA continues to encourage airport operators, via voluntary measures, to utilize biometrics in their credentialing and access control systems. As to establishing milestones, TSA will continue to work in collaboration with the airport industry toward the continued development and refinement of existing biometric airport access control standards. As noted in the draft report, TSA did work in collaboration with the industry, specific to development of biometric access control standards, which resulted in the publication of RTCA DO-230B, titled *Integrated Security System Standard for Airport Access Control,* dated June 19, 2008.

Recommendation 4: ***Develop milestones for establishing agency procedures for reviewing airport perimeter and access control requirements imposed through security directives.***

Concur: Milestones for establishing Agency procedures for reviewing airport perimeter and access control requirements imposed through security directives (SDs) are necessary. However, TSA must maintain its flexibility in processing those SDs, as some of the security issues addressed in these documents have greater implications than others. TSA has issued SDs as a means to immediately mitigate risk in the aviation sector. Over the years, there have



been risks that have arisen that required action in a manner quicker than the rule making process would allow. For example, the issuance of an SD limiting liquids, gels, and aerosols in commercial airport sterile areas, issued in August 2006, was developed as a result of intelligence revealing a direct and immediate threat to the traveling public. Unfortunately, that threat, like others, has not gone away, hence the need to sustain the SD. In more recent times, an SD was issued in December of 2008 on the subject of airport employee badging procedures. This directive had the U.S. Department of Homeland Security level impetus and was issued as a result of significant security issues identified nationwide at commercial airports. This SD was coordinated with industry through a non-disclosure procedure and reviewed before it was issued. In this instance, there was ample time to allow for that level of coordination.

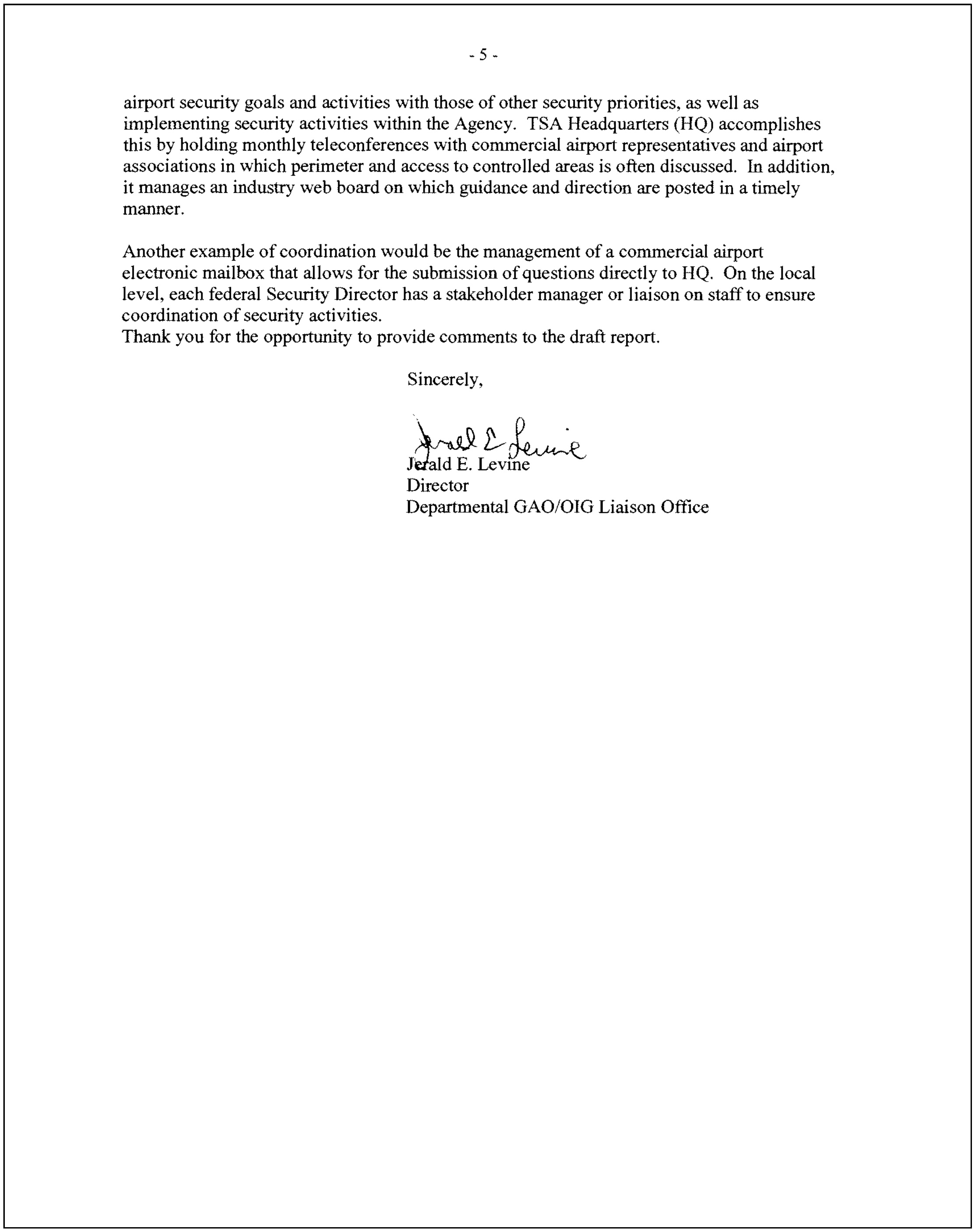
The SD issuance procedures include an internal TSA review and an evaluation of TSA's legal authority to issue SDs. The procedure also takes into consideration the industry's ability to carry out the security measures to mitigate the threat while continuing operations and meeting the needs of the public. SDs are revised as necessary, and reflective of changed conditions and/or airport stakeholder feedback.

Recommendation 5: ***To better ensure a unified approach among airport security stakeholders for developing, implementing, and assessing actions for securing airport perimeters and access to controlled areas, TSA should develop a national strategy for airport security that incorporates key characteristics of effective security strategies, including:***

- ***Measurable goals, priorities, and performance measures. TSA should also consider using information from other methods, such as covert testing and proxy measures, to gauge progress toward achieving goals.***
- ***Program cost information and the sources and types of resources needed. TSA should also indentify where those resource would be most effectively applied by exploring ways to develop and implement cost-benefit analysis to identify the most cost-effective alternatives for reducing risk.***
- ***Plans for coordinating activities among stakeholders, integrating airport security goals and activities with those of other aviation security priorities, and implementing security activities within the agency.***

Concur: TSA will accomplish this task by updating the Transportation Systems Sector Specific Plan, a document which subsumes the National Strategy for Transportation Security– which, in turn, includes airport security within its scope. This plan includes measurable goals, priorities, and performance measures, as well as cost information. TSA will socialize the document with its Sector Coordinating Councils (SCC) while it is in draft form, and will receive SCC concurrence before finalizing the document. TSA expects to release this updated document in the summer of 2010.

An example of TSA's efforts to work toward a national strategy is the Compliance and Enforcement Program supported by the Transportation Security Inspection (TSI) function. Inspections of commercial airports are conducted on a regular basis and are based on Title 49, Code of Federal Regulations (CFR), Part 1542, which outlines the security measures a commercial airport must implement for Federal compliance. To ensure compliance and to provide a foundation for our national strategy, TSA has initiated several mechanisms to



airport security goals and activities with those of other security priorities, as well as implementing security activities within the Agency. TSA Headquarters (HQ) accomplishes this by holding monthly teleconferences with commercial airport representatives and airport associations in which perimeter and access to controlled areas is often discussed. In addition, it manages an industry web board on which guidance and direction are posted in a timely manner.

Another example of coordination would be the management of a commercial airport electronic mailbox that allows for the submission of questions directly to HQ. On the local level, each federal Security Director has a stakeholder manager or liaison on staff to ensure coordination of security activities.
Thank you for the opportunity to provide comments to the draft report.

Sincerely,

Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

Appendix IX: GAO Contact and Staff Acknowledgments

GAO Contact

Stephen M. Lord (202) 512-4379 or lords@gao.gov

Acknowledgments

In addition to the contact named above, Steve Morris, Assistant Director, and Barbara Guffy, Analyst-in-Charge, managed this assignment. Scott Behen, Valerie Colaiaco, Dorian Dunbar, Christopher Keisling, Matthew Lee, Sara Margraf, Spencer Tacktill, Fatema Wachob, and Sally Williamson made significant contributions to the work. Chuck Bausell, Jr. provided expertise on risk management and cost-benefit analysis. Virginia Chanley and Michele Fejfar assisted with design, methodology, and data analysis. Thomas Lombardi provided legal support; Elizabeth Curda and Anne Inserra provided expertise on performance measurement; and Pille Anvelt developed the report's graphics.

(440624)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548